Superintendencia de Servicios Financieros

Estándares Mínimos de Gestión para Empresas Aseguradoras

Vigencia: 1 de julio de 2022

BANCO CENTRAL
DEL URUGUAY

Índice

ESTÁNDARES MÍNIMOS DE GESTIÓN PARA EMPRESAS ASEGURADORAS

INTRODUCCIÓN

Tal como se establece en el Marco Operativo (https://www.bcu.gub.uy/Servicios-Financieros-SSF/Paginas/Marco-Operativo.aspx), los objetivos de la función de supervisión son identificar en forma temprana las debilidades de las entidades supervisadas promoviendo su efectiva resolución e identificar los riesgos y tendencias para el conjunto del sistema financiero, a efectos de que la Superintendencia de Servicios Financieros pueda actuar oportunamente para minimizar tales riesgos.

En este sentido, la acción supervisora está orientada fundamentalmente a verificar que:

- las entidades cuentan con adecuados niveles de capital y liquidez que les permitan respaldar los riesgos asumidos,
- son gestionadas por personal idóneo,
- llevan a cabo su negocio de modo prudente,
- cuentan con un adecuado sistema de gestión de riesgos y mantienen un adecuado ambiente de control,
- el sano desempeño puede mantenerse en escenarios adversos futuros.

Asimismo, y a efectos de contar con un mecanismo que permita sintetizar los resultados de la evaluación, se ha definido una metodología denominada CERT. El objetivo del CERT es sintetizar la evaluación por componente y en forma general, de tres aspectos:

- si existe alguna debilidad en uno de los componentes que requiera atención prioritaria por parte de la institución
- en qué etapa de resolución se encuentra dicha debilidad
- el impacto potencial de la debilidad encontrada sobre la capacidad de la institución de mantener niveles de solvencia prudenciales en el corto plazo.

LA METODOLOGÍA CERT

La metodología CERT considera los siguientes componentes:

C – Gobierno Corporativo: el sistema a través del cual las instituciones son dirigidas, monitoreadas y controladas.

E – Evaluación Económica Financiera: la situación económica financiera de la institución se analiza haciendo hincapié en el nivel y calidad del patrimonio de la institución y su capacidad de respaldar los riesgos asumidos y proveer protección a los asegurados y beneficiarios.

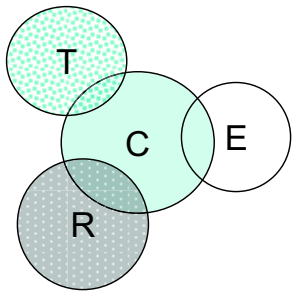
R – Riesgos: el sistema de gestión de riesgos de la institución y la capacidad de la misma de identificar, controlar, medir y monitorear los siguientes riesgos:

- Riesgo de Seguros
- Riesgo de Crédito
- Riesgo de Mercado
- Riesgo de Liquidez
- Riesgo Operacional
- Riesgo de Lavado de Activos y Financiamiento de Terrorismo
- Riesgo de Reputación
- Riesgo Estratégico

T – Tecnología: gestión de los riesgos tecnológicos y confiabilidad y eficacia de los sistemas de información como herramientas de la gestión.

Interrelación entre los distintos componentes del CERT

Desde el punto de vista metodológico debe visualizarse el Gobierno Corporativo como el núcleo central del análisis, con el cual se interrelacionan los otros componentes del sistema. Gráficamente, podemos verlo de la siguiente manera:



A los efectos de proveer orientación a las instituciones sobre cuáles son las expectativas del supervisor sobre los elementos mínimos que deben estar presentes en la gestión de las mismas, se presentan a continuación una serie de estándares mínimos de gestión asociados a los cuatro componentes de la metodología CERT.

Desde el punto de vista del supervisor se entiende que el no cumplimiento de un estándar constituye una debilidad que debe ser tratada con atención prioritaria por la entidad.

LOS ESTÁNDARES MÍNIMOS

Las empresas aseguradoras adoptan diferentes esquemas y estructuras para llevar adelante su gestión, tomando en cuenta la naturaleza, tamaño y complejidad de sus operaciones y su perfil de riesgos.

El supervisor lleva adelante sus procedimientos de supervisión y evaluación teniendo en cuenta estos elementos.

Se buscan evidencias de que los procesos y procedimientos, en general, son adecuados dadas las características de cada entidad y que las distintas estructuras de Gobierno Corporativo cumplen con sus roles y responsabilidades en forma adecuada.

Los hallazgos permiten a posteriori definir si existen o no apartamientos a los estándares que se definen seguidamente. El supervisor no certifica la adherencia estricta a los puntos específicos contenidos en estos estándares.

Definiciones

Marco de gestión de riesgos: incluye las políticas, procesos, controles y sistemas a través de las cuales se establece, comunica y monitorea el apetito de riesgo. Incluye además la declaración del apetito de riesgo, los límites de riesgo y un resumen de los roles y responsabilidades de los que supervisan la implementación y el monitoreo el apetito de riesgo. El marco debe tomar en cuenta los principales riesgos que enfrenta la institución y estar alineado con su estrategia y su plan de negocios.

Apetito de riesgo: El apetito de riesgo es el nivel y el tipo riesgo que una institución está dispuesta a asumir en sus exposiciones y actividades de negocio, teniendo en cuenta los objetivos definidos y las obligaciones con los accionistas y otras partes interesadas. El apetito de riesgo es generalmente expresado en términos cuantitativos y cualitativos y deben considerarse para definirlo la posibilidad de ocurrencia de condiciones y eventos extremos. El apetito de riesgo debe reflejar el potencial impacto en los resultados, el nivel de capital, el nivel de fondeo y la liquidez de la institución.

Declaración del apetito de riesgo: es el documento en el cual se establece el apetito de riesgo.

Límites de riesgo: Es la cantidad de riesgo aceptable relacionado a ciertos riesgos específicos o unidades específicas del negocio. Un sistema de límites debe incluir los límites de riesgo que no deben ser superados, de acuerdo con las políticas y los indicadores de alerta definidos.

Perfil de riesgo: valoración en un momento dado de las exposiciones al riesgo brutas de la institución o si procede exposiciones al riesgo netas.

Deber de diligencia: Deber de los miembros del Directorio de decidir y actuar con conocimiento de causa y prudencia en los asuntos de la institución. Suele interpretarse como la obligación de los directores de tratar los asuntos de la entidad como lo haría una «persona prudente» con sus asuntos personales.

Deber de lealtad - Deber de los directores de actuar de buena fe en el interés de la institución. El deber de lealtad debe impedir que cada director actúe en interés propio, o en el interés de otro individuo o grupo, a expensas de la institución sus accionistas y partes interesadas.

Conglomerado Financiero: conjunto o grupo formado por dos o más entidades interconectadas bajo un control común, o influencia significativa, de forma directa o indirecta, donde al menos alguna de ellas opera en algún sector regulado por la Superintendencia de Servicios Financieros.

ESTÁNDARES DE GOBIERNO CORPORATIVO (C)

El Gobierno Corporativo es el sistema a través del cual las instituciones son dirigidas, monitoreadas y controladas, comprende la Dirección, la Alta Gerencia y a los distintos mecanismos de control como son la Auditoría Interna, la Auditoría Externa y el Comité de Auditoría.

Un Gobierno Corporativo eficaz se basa en los siguientes componentes fundamentales:

- Cultura corporativa apropiada con normas establecidas para un comportamiento responsable y ético.
- Marco de apetito de riesgo.
- Responsabilidades bien definidas y comunicadas a toda la organización para la gestión de riesgos y controles, lo que se conoce como «las tres líneas de defensa»:
    - la línea de negocio,
    - una función de gestión del riesgo y de cumplimiento, independientes de la primera línea de defensa y
    - una función de auditoría interna independiente.

La línea de negocio –primera línea de defensa- es donde se generan primordialmente los riesgos y es responsable de su gestión continua.

La Gestión del riesgo -segunda línea de defensa- es responsable de identificar, medir, controlar y monitorear el riesgo, en forma independiente de la primera línea de defensa. La función de cumplimiento es también parte de esta segunda línea. Es responsable de realizar el seguimiento continuo del cumplimiento de la legislación, normas de gobierno corporativo, regulaciones, códigos y políticas a las que esté sujeta la institución.

La función de Auditoría Interna es la tercera línea de defensa. La misma debe realizar auditorías y revisiones independientes de las dos líneas anteriores, para garantizar al Directorio que el marco de gobierno general, incluido el marco de gestión de riesgos, es eficaz y que existen y se aplican consistentemente las políticas y procesos definidos.

- Existencia de una clara definición de roles y responsabilidades dentro de la organización que permita establecer sus objetivos, determinando los medios para alcanzarlos y cómo supervisar su cumplimiento. La estructura organizacional debe permitir a la Dirección implementar una estrategia eficiente y efectiva para la institución, asegurar al mismo tiempo un fuerte control interno, un buen sistema de administración de riesgos, un sistema contable que garantice integridad y confiabilidad y un sistema de información íntegro, oportuno y de fácil acceso.

- Integración del Directorio y la Alta Gerencia por personas con los conocimientos y competencias necesarias para cumplir sus roles respectivos. Deben *definir los objetivos estratégicos* planificar, dirigir la gestión comercial, de riesgos, monitorear los resultados, incluyendo la solvencia y las reservas técnicas, según los roles que se explicitan en los apartados correspondientes.

- Debe existir un ambiente de control adecuado y promover una cultura de riesgos en relación al volumen y complejidad de las operaciones y al perfil de riesgo de la institución. El mismo debe permitir un control eficiente y alentar un uso eficaz de los recursos.

Se considerarán en este capítulo los estándares mínimos que deben cumplir el Directorio, la Alta Gerencia, el Comité de Auditoría, la Auditoría Interna y la Auditoría Externa para asegurar un adecuado funcionamiento del Gobierno Corporativo.

DIRECTORIO

En adelante, cuando se habla del Directorio debe entenderse como el órgano responsable de la administración efectiva de la entidad.

El Directorio es el responsable último de definir la estrategia de negocios y controlar su implementación, vigilar la solvencia de la institución, tomar las decisiones sobre el personal clave, la organización interna y las prácticas de gobierno, fijar el apetito de riesgo y controlar la gestión del riesgo así como la suficiencia de las reservas técnicas y el cumplimiento de las obligaciones legales y regulatorias. También es responsable de asegurar la implementación de un sistema de remuneración con los incentivos adecuados.

El cuidado, diligencia, habilidad y prudencia con la cual los integrantes del Directorio cumplen sus roles tiene una influencia crítica sobre la viabilidad,

seguridad y solidez de la institución, sobre su capacidad de ejecutar la estrategia de negocio y cumplir los objetivos y sobre su capacidad de generar confianza a los asegurados y beneficiarios, supervisores y otros actores.

Los estándares mínimos que el Directorio debe cumplir son los que se detallan a continuación:

1. *El Directorio debe mantener una estructura apropiada que permita una visión independiente de la influencia de la Alta Gerencia, de influencias políticas y/o de otros intereses externos*.

Para ello:

1.1 El Directorio (3 miembros como mínimo) debe incluir personas con un buen balance de habilidades, experiencia y conocimientos, que de forma colectiva posean las aptitudes necesarias conforme al tamaño, complejidad y perfil de riesgo de la institución.

1.2 El Directorio debe estar integrado por un número suficiente de directores independientes[1] y directores No Ejecutivos[2]. Los Directores No Ejecutivos no deben tener injerencia en las decisiones diarias de la gestión.

1.3 Los Directores Ejecutivos no deben ejercer una influencia dominante en el conjunto del Directorio.

1.4 Los integrantes del Directorio deben tener un claro entendimiento de su rol dentro del Gobierno Corporativo y deben cumplir con el deber de lealtad y diligencia.

1.5 El Directorio debe poseer la capacidad de ejercer un juicio independiente sobre los asuntos de la institución. Ello no obsta a que el Directorio pueda participar en el proceso de aprobación de algunas operaciones o en algunas decisiones operativas de significativa magnitud para la entidad.

1.6 El Directorio debe implementar una estructura de Comités de Dirección acorde con el volumen, complejidad de las actividades y perfil de riesgos de la entidad para asegurar la participación de los distintos sectores involucrados en las decisiones relevantes.

[1] **Director independiente**: miembro no ejecutivo del Directorio sin responsabilidades de gestión en la institución y que no se encuentra sometido a ninguna influencia interna o externa, política o de propiedad, que le pudiera condicionar su opinión sobre los asuntos en los que debe intervenir. Será de aplicación para empresas aseguradoras privadas.

[2] **Director No Ejecutivo**: Si bien no existe desde el punto de vista jurídico el concepto de Director No Ejecutivo, debe entenderse por tal a aquellos Directores que no cumplen ninguna función ejecutiva, aunque mantienen sus responsabilidades como Directores.

1.7 El Directorio y sus Comités deben mantener documentadas y firmadas sus deliberaciones y decisiones (por ejemplo, actas de reuniones o resúmenes de temas tratados, recomendaciones emitidas, decisiones adoptadas y reportes utilizados para la toma de decisiones).

1.8 Las empresas aseguradoras con una participación de mercado[3] mayor al 10% deberán contar con un Comité de Riesgos a nivel del Directorio.

2. *El Directorio debe asegurar un adecuado relacionamiento con el accionista o con la entidad controlante.*

Para ello el Directorio debe asegurar que:

2.1 Existe una adecuada coordinación e integración entre la entidad y su controlante.

2.2 Existe un adecuado control y monitoreo sobre las actividades tercerizadas, cuando sean realizadas por empresas relacionadas.

2.3 Sus roles y responsabilidades y los de su controlante y vinculadas se encuentran claramente establecidos y delimitados.

2.4 Su independencia es respetada por parte de su controlante en lo que refiere a las responsabilidades que debe asumir el Directorio.

3. *El Directorio debe seleccionar, monitorear y si es necesario reemplazar a la Alta Gerencia.*

Para ello, el Directorio debe:

3.1 Aprobar los roles y responsabilidades de la Alta Gerencia.

3.2 Evaluar si el conocimiento, integridad y experiencia de la Alta Gerencia siguen siendo apropiados dada la naturaleza del negocio y el perfil de riesgo de la institución.

3.3 Evaluar regularmente la efectividad y prudencia de la Alta Gerencia en la gestión de las operaciones y de los riesgos, revisando de forma crítica las explicaciones e información facilitada.

3.4 Asegurar que la Alta Gerencia que se designe cumple con los criterios de capacidad e integridad y que sus actuaciones son coherentes con la

[3] La participación de mercado se mide en función de las primas retenidas netas devengadas, excluyendo ADT y Seguros previsionales.

estrategia y políticas aprobadas por Directorio, incluidos sus valores, cultura y apetito de riesgo y establecer las posibles consecuencias si dichas acciones no se alinean con las expectativas de desempeño.

3.5 Aprobar un plan de sucesión para el equipo gerencial.

4. *El Directorio debe aprobar los objetivos estratégicos de la institución y supervisar su implementación, tanto a nivel individual como en base consolidada, cuando corresponda.*

Para ello, el Directorio debe:

4.1. Aprobar un Plan estratégico adecuado al nivel de capital de la empresa que defina claramente el negocio objetivo y los retornos esperados y que éstos sean consistentes con el apetito de riesgo definido. Este marco debe estar claramente plasmado en políticas escritas y comunicado a toda la institución.

4.2. Aprobar el Plan de Negocios que contemple los objetivos estratégicos definidos, dentro de los cuales se contemplarán los negocios de las distintas entidades que componen el Conglomerado, cuando corresponda.

4.3. Evaluar regularmente los resultados comparándolos contra el presupuesto aprobado.

4.4. Revisar por lo menos anualmente los objetivos estratégicos, los planes, el apetito de riesgo y los límites de riesgo para asegurar que siguen siendo válidos.

4.5. Asegurar la existencia de un sistema de información íntegro, confiable y oportuno que permita tomar sus decisiones y que asegure la efectividad del mismo.

4.6. Aprobar una estrategia y políticas de Tecnología de la Información (TI), adecuadas a la estrategia general de la empresa y asegurar que la Alta Gerencia implementa los procedimientos que las hacen aplicables. Para lo cual debe asegurar que:

- La Institución cuenta con una organización y con personal capacitado para una adecuada gestión de TI y de los riesgos asociados.
- El soporte de TI permite dar cumplimiento a los requerimientos legales, regulatorios, contractuales y operativos para el manejo de riesgos.

4.7. Aprobar una estrategia y política de Seguridad de la información adecuadas a la estrategia general de la institución y asegurar que la Alta Gerencia implemente los procedimientos que las hacen aplicables.

5. *El Directorio debe aprobar un marco de gestión de riesgos que contenga la declaración de apetito de riesgo consistente con los objetivos estratégicos, los límites de riesgo y políticas asociadas que permitan la identificación, medición, monitoreo y control de todos los riesgos que puedan afectar el cumplimiento de los objetivos de la entidad, tanto en base individual como a nivel consolidado, cuando corresponda.*

Para ello el Directorio debe:

5.1. Entender los riesgos que enfrenta la entidad, así como definir el nivel de exposición a cada tipo de riesgo.

5.2. Promover una cultura de riesgos en la organización.

5.3. Aprobar el marco de gestión de riesgos que incluya la declaración del apetito de riesgo y revisarlo al menos anualmente, así como los roles y responsabilidades asociados y los mecanismos de medición y seguimiento.

La declaración del apetito de riesgo debe

- Ser consistente con la estrategia general, el perfil general de riesgo y el Plan de Negocios definidos y su tolerancia con los riesgos que se quiere asumir.
- Considerar los factores internos y externos que afectan la entidad, (aspectos coyunturales de la economía, su posición en el mercado, las ramas o productos en que opera, las capacidades del personal, la tecnología, etc.).
- Estar claramente definida por escrito y ser coherente con prácticas aseguradoras prudentes y con los requisitos regulatorios.

5.4. Asegurar que la Alta Gerencia implementa un sistema de gestión de riesgos que contemple el apetito de riesgo definido por el Directorio y que involucra a todo el personal.

5.5. Asegurar que cuenta con los recursos requeridos para gestionar los riesgos dentro del marco establecido.

5.6. Asegurar que existan políticas y procedimientos por escrito que constituyan una guía efectiva para asumir y gestionar los riesgos y que dichos procedimientos estén implementados previo a la realización de nuevas actividades o al lanzamiento de nuevos productos.

5.7. Asegurar que la Alta Gerencia toma las medidas necesarias para implementar una gestión de proyectos efectiva.

5.8. Asegurar que existe una gestión de TI y de la seguridad de la información cuyos objetivos se encuentran alineados con los del negocio.

5.9. Asegurar que existe un sistema de Evaluación de Riesgos que garantiza el logro de los objetivos de TI y de seguridad de la información de la entidad que permita responder a las amenazas.

5.10. Asegurar que los procesos relevantes (entre ellos suscripción, tarificación, inversiones, reservas técnicas y TI) se monitorean y son auditados regularmente por personas independientes.

5.11. Asegurar que la institución cuenta con un plan de continuidad del negocio adecuado al volumen, naturaleza y complejidad de sus operaciones y que, en particular, incluya un plan de contingencia de TI.

6. *El Directorio debe asegurar que la función actuarial cumple su cometido.*

La función actuarial comprende la participación en:

- la definición de las políticas de riesgo de seguro y en el lanzamiento de nuevos productos,
- la gestión de los riesgos propios de los seguros,
- la determinación y valuación de las reservas técnicas.

Sin perjuicio de esto, la responsabilidad última sobre estos aspectos recae sobre el Directorio de la Institución.

Para ello el Directorio debe:

6.1. Reconocer la importancia de esta función asignando los recursos necesarios para un adecuado desempeño de la misma.

6.2. Asegurar que esta función es llevada a cabo por personal independiente del área comercial.

6.3. Asegurar que quien realice la función cuenta con la competencia y capacidad necesaria para cumplir su función adecuadamente.

6.4. En el caso que dicha función se tercerice se deberá asegurar que se cumplan los estándares anteriormente detallados.

7. *El Directorio debe promover una cultura corporativa que exija y provea los incentivos adecuados para una conducta ética y que evite o administre los posibles conflictos de interés.*

Para ello el Directorio debe:

7.1. Establecer y comunicar los estándares éticos (a través de un Código de Ética) que guíen el accionar de la institución.

7.2. Definir una política sobre conflictos de intereses y un procedimiento de cumplimiento para su aplicación.

7.3. Actuar como ejemplo del cumplimiento de los estándares éticos.

7.4. Asegurar que la Alta Gerencia implementa políticas y procedimientos adecuados para evitar o administrar los posibles conflictos de interés y confirmar que los empleados y la Alta Gerencia son conscientes de que se tomarán medidas disciplinarias u otras medidas apropiadas ante comportamientos inaceptables o infracciones.

7.5. Asegurar que existen políticas y procedimientos claramente definidos para el tratamiento de operaciones con partes relacionadas para que todas las transacciones se realicen en condiciones de equidad o mercado y se adopten códigos de gobierno corporativo adecuados. Estas políticas deberían incluir la aprobación por parte del Directorio de las operaciones más significativas (excluyendo a los Directores que pueden tener conflictos de interés).

7.6. Asegurar que las políticas de remuneración y compensación, incluidas las comisiones por intermediación, son transparentes y consistentes con la estrategia global de largo plazo de la institución, la cultura y el apetito de riesgo y que existen mecanismos para verificar su cumplimiento. El sistema de remuneración debe crear los incentivos necesarios para gestionar en forma adecuada el riesgo y el capital.

7.7. Vigilar la integridad, independencia y eficacia de las políticas y procedimientos de denuncia de irregularidades de la institución.

8. *El Directorio debe promover una cultura de control en la organización, verificando que la Alta Gerencia implementa las políticas y procedimientos necesarios para que todos entiendan su rol en el control interno y la gestión de riesgos.*

Para ello, el Directorio debe:

8.1. Promover una cultura de riesgo y transmitir que todos los empleados son responsables de ayudar a la institución a operar dentro del grado de apetito de riesgo y las delimitaciones del riesgo establecidas.

8.2. Aprobar la estructura organizativa acorde al tamaño, complejidad, naturaleza y volumen de las operaciones y al perfil de riesgos de la institución y asegurar que la misma es conocida por toda la organización. Esta estructura debe asegurar:

- Una clara separación y equilibrio de las funciones comerciales y de toma de riesgos de las funciones de monitoreo y control.
- Que existan sendas funciones de riesgo y de cumplimento claramente definidas e independientes de la gestión, contando con la suficiente autoridad, relevancia, recursos y acceso al Directorio.
- Que existe una adecuada segregación de funciones que facilite los controles cruzados.
- Que exista una función de Auditoría Interna, independiente de la gestión, que cuente con la suficiente autoridad, relevancia, recursos y acceso al Directorio.

8.3. Asegurar que existen mecanismos de control interno efectivos, acorde a la naturaleza y complejidad de las operaciones.

8.4. Asegurar que existe una clara definición de deberes y responsabilidades que sea consistente con la estrategia definida y que permita una clara asignación de autoridad.

8.5. Controlar a la Alta Gerencia en la implementación de las estrategias y el cumplimiento de las políticas establecidas.

8.6. Asegurar que el nivel de control se mantiene aún en el caso de tareas tercerizadas.

8.7. Asegurar que el sistema de información sea oportuno, íntegro y confiable. En particular, el Comité de Auditoría o la Auditoría Interna deberán cerciorarse que la información para la toma de decisiones es adecuada.

9. *El Directorio debe asegurar que el Comité de Auditoría cumple su cometido.*

Para ello, el Directorio debe:

9.1. Aprobar un estatuto o misión que establezca el propósito del Comité, sus objetivos, organización, autoridad y responsabilidad, así como las características que debe tener el registro donde consten los temas tratados en cada reunión del Comité de Auditoría

9.2. Asegurar que la integración de este Comité de Dirección es acorde con la naturaleza, complejidad y volumen de las operaciones de la institución y que permite cumplir su cometido con independencia. Para ello, la mayoría de los miembros no deben estar involucrados con la gestión diaria de la entidad.

9.3. Asegurar que la experiencia de todos sus miembros es compatible con sus obligaciones.

9.4. Proveer al Comité de Auditoría de apoyo y recursos para que pueda desempeñar sus funciones en forma independiente.

9.5. Asegurar que la periodicidad de las reuniones es suficiente para monitorear y evaluar el adecuado funcionamiento de los mecanismos de control interno.

9.6. Tener comunicación regular con el Comité de Auditoría promoviendo la rápida resolución de debilidades encontradas.

10. *El Directorio debe asegurar que la función de Auditoría Interna cumple su cometido.*

Para ello el Directorio debe:

10.1. Asegurar que la Auditoría Interna –propia o tercerizada- es independiente de las actividades auditadas y que cuenta con la suficiente autoridad y jerarquía para poder actuar con objetividad e imparcialidad.

10.2. Asegurar que la línea de reporte es a sí mismo o al Comité de Auditoría

10.3. Asegurar que la función de Auditoría Interna es llevada a cabo por personal independiente, competente y capacitado y que existen recursos suficientes para cumplir con los objetivos establecidos y el plan anual.

10.4. Asegurar, en forma directa o a través del Comité de Auditoría, que el Auditor Interno cumple con sus cometidos con eficacia y eficiencia.

10.5. Asegurar el acceso de la Auditoría Interna a la información necesaria para ejercer su función con eficacia

10.6. Asegurar que la Alta Gerencia toma las medidas necesarias para corregir los problemas deficiencias o debilidades encontradas por la Auditoria Interna.

11. *El Directorio debe asegurar que la Auditoría Externa cumple su cometido.*

Para ello, el Directorio debe:

11.1. Reconocer y comunicar la importancia de la función de Auditoría Externa dentro de la organización.

11.2. Tomar las medidas necesarias para asegurar la independencia de la Auditoría Externa dentro de la organización.

11.3. Asegurar que la Alta Gerencia toma las medidas necesarias para corregir los problemas detectados oportunamente.

12. *El Directorio debe asegurar que la institución cuenta con un nivel de reservas técnicas para hacer frente a las reclamaciones y gastos esperados, y de capital para hacer frente a las pérdidas inesperadas (no cubiertas por las reservas técnicas) y los demás riesgos a los que se encuentra expuesta, protegiendo así los derechos de los asegurados y beneficiarios.*

Para ello el Directorio debe:

12.1. Implementar un proceso sistemático e integral para determinar el nivel y calidad de capital y la suficiencia de las reservas técnicas, tomando en cuenta factores tales como:
- La estrategia de negocios actual y futura.
- El perfil de riesgos y apetito de riesgo
- La capacidad del capital de absorber pérdidas por eventos no anticipados e incertidumbre en los propios sistemas de medición.

12.2. Asegurarse que el capital y las reservas técnicas cumplan con los requisitos regulatorios.

13. *El Directorio debe asegurar que la información provista al Supervisor representa fielmente la situación económico-financiera y los riesgos asumidos*

Para ello, el Directorio debe asegurar que:

13.1. Los procesos de elaboración de información son confiables

13.2. La contabilidad se realice de acuerdo con los criterios establecidos en la normativa existente.

13.3. Todos los hechos relevantes que pudieran impactar negativamente a la institución son informados al Supervisor oportunamente.

ALTA GERENCIA

Las responsabilidades de la Alta Gerencia se centran en la implementación de las políticas, procedimientos, procesos y controles necesarios para gestionar las operaciones y riesgos en forma prudente para cumplir con los objetivos estratégicos y el apetito de riesgo fijados por el Directorio. Se debe asegurar que el Directorio recibe información relevante, íntegra y oportuna que le permita evaluar la gestión y analizar si las responsabilidades delegadas a la Alta Gerencia se están cumpliendo efectivamente.

En general, debe entenderse como Alta Gerencia al equipo formado por la Gerencia General o similar y las líneas de reporte relevantes, quienes en su conjunto son los responsables de la ejecución de la estrategia de la institución.

Los estándares mínimos que la Alta Gerencia debe cumplir son los que se detallan a continuación:

14. La Alta Gerencia como equipo y cada uno de sus integrantes deben poseer los conocimientos y habilidades para gestionar y supervisar la actividad, de conformidad con la estrategia, el plan de negocios, el apetito de riesgo y otras políticas aprobadas por el Directorio.

Para ello, la Alta Gerencia debe:

14.1 Estar integrada por personas con la capacidad, experiencia e integridad necesarias para gestionar las actividades y el personal bajo su supervisión.

14.2 Trabajar como equipo respetando los roles de los distintos integrantes y asegurar el cumplimiento de las directivas establecidas por el Directorio.

14.3 Ejercer una adecuada vigilancia de sus subordinados y garantizar que las actividades de la institución sean coherentes con la estrategia definida, así como con el apetito de riesgo y las políticas aprobadas por el Directorio.

14.4 Contar con acceso regular a capacitación para mantener, mejorar sus competencias en las áreas de su responsabilidad y mantenerse al tanto de los desarrollos relevantes para sus áreas de responsabilidad.

15. La Alta Gerencia debe establecer y seguir un proceso continuo y adecuado para la gestión estratégica de la entidad en función de los lineamientos del Directorio y rendir cuentas a éste de lo actuado.

Para ello, la Alta Gerencia debe:

15.1 Desarrollar y presentar al Directorio para su aprobación:

- El plan de negocios en base a los lineamientos estratégicos y a la declaración de apetito de riesgo definidos por el Directorio, que considere las características del entorno económico y de negocios, la situación económico - financiera y patrimonial de la institución y los riesgos en los cuales tiene o tendrá exposiciones.
- El presupuesto anual.
- El plan de continuidad del negocio de acuerdo a los lineamientos estratégicos definidos por el Directorio en materia de resiliencia operativa.

15.2 Implementar la estrategia y el plan de negocios aprobado.

15.3 Asegurar que la estructura organizacional es consistente con los objetivos estratégicos y políticas aprobadas por el Directorio.

15.4 Monitorear periódicamente el cumplimiento con respecto al presupuesto y al plan de negocios y analizar los desvíos.

15.5 Proveer al Directorio de información completa, relevante, oportuna y con una periodicidad adecuada, al menos sobre los siguientes temas:

- la implementación de la estrategia y los planes,
- propuestas de modificaciones en la estrategia de negocios, en la estrategia de riesgos o apetito de riesgo, ante cambios en el entorno que así lo ameriten,
- los resultados y condición financiera de la institución, comparación de resultados reales contrastados con los proyectados,
- excepciones a los límites del riesgo y/o infracciones a las normas de cumplimiento,
- suscripción, reservas y reaseguros,
- deficiencias en los controles internos,
- inquietudes jurídicas o regulatorias,
- denuncias de irregularidades,
- resultados de las pruebas del plan de continuidad

15.6 Poner en práctica las políticas de compensación fijadas por el Directorio.

16. La Alta Gerencia debe implementar un sistema de gestión integral de riesgos que contemple el apetito de riesgo, involucre a todo el personal y sea proactivo.

Para ello, la Alta Gerencia debe:

16.1 Implementar la estrategia de riesgos aprobada por el Directorio.

16.2 Asegurar que existe un responsable del manejo de cada uno de los riesgos y un sistema que permita obtener una visión integral de los riesgos que asume la entidad.

16.3 Desarrollar, poner en práctica y hacer cumplir los procesos y procedimientos que permitan identificar, medir, monitorear y controlar todos los riesgos que puedan afectar el cumplimiento de los objetivos de la institución.

16.4 Asegurar que cuenta con los recursos suficientes para un manejo adecuado y ajustado al marco de riesgos definido por la Dirección.

16.5 Asegurar que el personal involucrado en el proceso de Gestión de Riesgos tiene la capacidad técnica para comprender y analizar los riesgos asumidos. La descripción de funciones, cargos y responsabilidades del personal involucrado deberá incluir explícitamente el rol en el sistema de gestión integral de riesgos.

16.6 Definir e implementar un marco de gestión de proyectos basado en mejores prácticas.

16.7 Implementar un proceso para la aprobación y puesta en producción de nuevas ramas o productos que asegure un adecuado control y gestión de riesgos antes de su implementación.

16.8 Implementar procedimientos sobre las políticas de seguridad de la información aprobadas por el Directorio.

16.9 Asegurar que existe un sistema de revisión independiente de los procesos y procedimientos de riesgos para identificar y resolver debilidades.

16.10 Evaluar y revisar en forma periódica los riesgos a los que se expone la entidad, así como su perfil general de riesgos reportándolo oportunamente al Directorio.

17. La Alta Gerencia debe promover una cultura de control en toda la organización.

Para ello, la Alta Gerencia debe:

17.1 Diseñar y mantener una estructura organizacional de acuerdo a los lineamientos aprobados por el Directorio, que asegure un adecuado sistema de control.

17.2 Diseñar un sistema de comunicación que asegure que todo el personal de la institución entiende y cumple su rol en el control interno.

17.3 Asegurar la existencia de comités u otros mecanismos que aseguren una efectiva coordinación y comunicación entre las distintas áreas de la empresa y que promuevan la transparencia y rendición de cuentas.

17.4 Asegurar que los comités existentes mantengan adecuadamente documentadas sus deliberaciones y decisiones (por ejemplo, actas de reuniones o resúmenes de temas tratados, recomendaciones y decisiones adoptadas).

17.5 Demostrar en su actuación diaria un claro compromiso con el control.

17.6 Mantener un seguimiento estricto de los riesgos derivados de las actividades tercerizadas, asegurando la calidad del sistema de control de la institución.

17.7 Tomar las medidas necesarias para corregir los problemas detectados por el Auditor Interno, Externo y el Supervisor

17.8 Facilitar el relacionamiento con el supervisor y proveer los elementos necesarios para que éste pueda cumplir su rol.

17.9 Proporcionar al Directorio la información que necesite para efectuar sus funciones de supervisión de la Alta Gerencia y evaluar la calidad de su desempeño.

18. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio para evitar o administrar posibles conflictos de interés y establecer los procedimientos de control necesarios.

Para ello, la Alta Gerencia debe:

18.1 Implementar las políticas y procedimientos para identificar, evitar o administrar y explicitar adecuadamente los conflictos de interés, en particular, en lo vinculado a las operaciones con entidades relacionadas.

19. La Alta Gerencia debe implementar un proceso íntegro de gestión de la Tecnología de Información (TI) consistente con la estrategia.

Para ello se debe cumplir que:

19.1 Los roles del responsable del área de TI se encuentran claramente definidos.

19.2 Existen políticas de medición y mitigación de los riesgos en los procesos.

19.3 Se entiende y se comunica la necesidad de cumplir con los requerimientos del organismo supervisor.

19.4 La responsabilidad de TI está ubicada dentro de la estructura general de la organización de modo de garantizar la competencia técnica e independencia respecto de las áreas usuarias, para garantizar soluciones, de tecnología de la información, útiles para la organización.

19.5 El área de TI tenga la habilidad de desarrollar, adquirir, instalar y mantener soluciones apropiadas y acordes a las necesidades de la entidad, en forma prudente y dentro de un ambiente controlado.

19.6 Existen procedimientos de control de la gestión de TI. Los servicios a ser prestados por el área de TI deben ser monitoreados por la Alta Gerencia y comparados con los niveles mínimos establecidos (indicadores clave de desempeño y/o factores críticos de éxito). La evaluación del desempeño del área de TI debe llevarse a cabo en forma continua.

19.7 La Alta Gerencia, a intervalos regulares, mide la satisfacción del cliente sobre los servicios prestados por TI para identificar el déficit en los niveles de servicio y establecer objetivos de mejoras.

19.8 Los procesos que no alcancen las metas mínimas de desempeño establecidas, se deberán seleccionar para ser incluidos en procesos de mejoras.

19.9 Se ejecutan los procedimientos implementados por la Alta Gerencia, sobre las políticas de seguridad de la información aprobadas oportunamente por el Directorio.

20. La Alta Gerencia debe definir e implementar un sistema de información adecuado para cuantificar, evaluar y notificar al Directorio el volumen, composición y calidad de las exposiciones de los riesgos que asume la entidad. La información debe ser confiable, oportuna, fácilmente accesible y provista en un formato consistente.

El sistema de información debe:

20.1 Cubrir todas las actividades significativas de la institución.

20.2 Estar integrado por información técnica, financiera, operativa y de cumplimiento, adecuada y completa. Se deberá explicitar el sistema de

reportes que incluya tanto los reportes utilizados internamente, como los que se emiten para terceras partes.

20.3 Incluir información sobre eventos externos y condiciones relevantes a la toma de decisiones.

20.4 Cumplir con las características de:

- **Oportunidad** – El sistema debe proveer información actualizada en forma oportuna a los usuarios apropiados, de forma de facilitar la toma de decisiones.
- **Precisión** – El sistema de controles sobre el procesamiento de información debe ser efectivo.
- **Consistencia** – La información debe ser procesada y compilada en forma consistente y uniforme. Los cambios en los sistemas deben estar adecuadamente documentados y claramente comunicados a los usuarios de la información.
- **Integridad** – Los tomadores de decisiones deben contar con información completa y pertinente en forma sintetizada.
- **Relevancia** - La relevancia de la información está directamente relacionada con las necesidades de la Gerencia y la Dirección para el desarrollo de su trabajo.

20.4 El proceso de generación de información debe ser seguro, estar independientemente monitoreado y respaldado con planes de contingencia adecuados.

20.5 Los informes remitidos al organismo supervisor deben proveer datos confiables, para lo cual se deben verificar previamente.

20.6 Cuando la institución utilice modelos para medir los riesgos, se deben realizar validaciones periódicas e independientes de los mismos.

COMITÉ DE AUDITORÍA

21. El Comité de Auditoría debe asegurar que el sistema de gestión integral de riesgos de la institución es adecuado y que se toman las medidas necesarias para su mantenimiento en forma continua.

Para ello, el Comité de Auditoría debe:

21.1 Estar conformado adecuadamente de forma de asegurar el cumplimiento de los objetivos fijados para esta estructura de control, en el que participe el Director independiente, contando con al menos un Director no ejecutivo.

21.2 Reunirse con una periodicidad acorde a la naturaleza, tamaño y complejidad de las operaciones de la institución y a su perfil de riesgos, y documentar adecuadamente todas sus decisiones y deliberaciones (por ejemplo, actas de reuniones o resúmenes de temas tratados, recomendaciones emitidas y decisiones adoptadas).

21.3 Hacer un seguimiento de las acciones correctivas llevadas a cabo por la Alta Gerencia para subsanar las observaciones de la Auditoría Interna, Externa y del Supervisor de manera oportuna y monitorear su implementación.

21.4 Proveer información al Directorio que le permita evaluar el desempeño del Comité de Auditoría y sus preocupaciones.

21.5 Vigilar regularmente el adecuado funcionamiento de los mecanismos de control interno, así como verificar que se establezcan las medidas correctivas tendientes a corregir las debilidades detectadas y monitorear su implementación.

21.6 Asegurar que la Alta Gerencia establece y mantiene un adecuado y efectivo sistema de gestión integral de riesgos.

21.7 Implementar un proceso orientado a identificar áreas de riesgo donde se debe profundizar las tareas de Auditoría y documentar sus resultados por lo menos anualmente.

21.8 Aprobar un documento que establezca el propósito de la Auditoría Interna, sus objetivos, su autoridad y responsabilidades, así como un manual de procedimientos para el trabajo de Auditoría.

21.9 Analizar y aprobar el plan y cronograma anual de Auditoría Interna y monitorear su funcionamiento y desempeño en el cumplimiento de los planes de Auditoría oportunamente aprobados.

21.10 Aprobar la contratación y honorarios de los auditores externos e informar al Directorio. Esta contratación también puede ser realizada por el propio Directorio.

21.11 Revisar el plan de trabajo de la Auditoría Externa y sus resultados, y efectuar un seguimiento de la independencia y eficacia del Auditor Externo asegurando que otras tareas adicionales (por ejemplo, consultorías) son compatibles y no impactan negativamente su independencia.

21.12 Revisar los informes de la Auditoría Externa, Auditoría Interna y del Supervisor así como tomar conocimiento de los Estados Contables y toda otra información relevante de la entidad.

21.13 Acceder a los resultados obtenidos por el Síndico o la Comisión Fiscal en la realización de sus tareas, según surja de sus respectivos informes.

21.14 Establecer una comunicación eficaz con el Auditor Externo y exigirle que informe sobre todos los asuntos pertinentes que permita a dicho comité desempeñar sus responsabilidades de vigilancia y mejorar la calidad de la auditoría.

21.15 Mantener comunicación periódica con la Superintendencia de Servicios Financieros a fin de conocer sus inquietudes, los problemas detectados en la supervisión de la institución, así como el seguimiento llevado a cabo para su solución.

21.16 Revisar las políticas establecidas en la institución relativas al cumplimiento de leyes y regulaciones, normas de ética, conflictos de intereses e investigaciones por faltas disciplinarias y fraude.

AUDITORÍA INTERNA

22. La función de Auditoría Interna debe proporcionar fiabilidad al Directorio y al Comité de Auditoría sobre la calidad y eficacia de los sistemas y procesos de control interno, gestión del riesgo, cumplimiento y gobierno corporativo de la institución, ayudando con ello al Directorio y Comité de Auditoría a proteger su organización y reputación.

Para el cumplimiento de este estándar, se considera que la función de Auditoría Interna debe:

22.1 Tener un mandato claro, rendir cuentas al Directorio y al Comité de Auditoría, debiendo actuar con objetividad, imparcialidad e independencia funcional de las restantes áreas que conforman la estructura organizativa de la institución, para lo cual debe contar con suficientes recursos y autoridad para desempeñar sus funciones de forma eficaz y objetiva.

22.2 Contar con los conocimientos y experiencia adecuados, en forma individual y colectiva.

22.3 Cumplir con los estándares y prácticas internacionales de auditoría interna y con el código de ética pertinente.

22.4 Elaborar y someter a la aprobación del Comité de Auditoría un documento que establezca sus objetivos, funciones, autoridad y responsabilidades, así como un manual de procedimientos para realizar su trabajo, el cual deberá aplicarse en caso de tercerización de tareas de Auditoría Interna.

22.5 Implementar procesos que aseguren que las pruebas, hallazgos y acciones correctivas son documentados adecuadamente y realizar un seguimiento proactivo de las debilidades encontradas.

22.6 Desarrollar y presentar al Comité de Auditoría un plan anual de Auditoría basado en riesgos. El plan anual debe contener el alcance, los ciclos a auditar con su valoración de riesgo, cronogramas, recursos humanos necesarios y sistema de reportes, debiendo cubrir todas las actividades de la entidad (incluso las tercerizadas) en los ciclos previstos.

22.7 Debe evaluar la efectividad y eficiencia, al menos de:

- el sistema de gestión integral de riesgos,
- las medidas adoptadas para la implementación del marco de apetito de riesgo definido por el Directorio,
- el sistema de información gerencial y sus procesos,
- Los procesos de suscripción, constitución de reservas y reaseguros,
- El diseño e implementación del enfoque de resiliencia operativa,
- los procesos de TI y de gestión de seguridad de la información,
- los controles internos,
- la precisión y confiabilidad de los registros contables y los informes financieros y de gestión,
- los sistemas diseñados para asegurar el cumplimiento de los requisitos legales, normativos y contractuales, así como del código de ética,
- la comprobación de la fiabilidad y oportunidad de los informes exigidos por el Supervisor,
- el seguimiento de las recomendaciones efectuadas.

22.8 Implementar el plan aprobado e informar al Comité de Auditoría sobre la existencia de desvíos significativos y el impacto de dichos desvíos sobre el cumplimiento de los objetivos establecidos.

22.9 Presentar sus informes de actuación con sus conclusiones y recomendaciones al Comité de Auditoría para su información y acción.

22.10 Mantener un inventario de debilidades encontradas, la fecha inicial de hallazgos y las medidas adoptadas para su corrección, así como su seguimiento.

22.11 Mantener estrecha coordinación con otras estructuras de control (Síndico, Comisión Fiscal, etc.) que aseguren la cobertura de todas las actividades de la entidad.

AUDITORÍA EXTERNA

23. La Auditoría Externa debe aportar una seguridad razonable de que los estados financieros en su conjunto están libres de incorrección material, debido a fraude o error y que están preparados, en todos los aspectos materiales, de conformidad con el marco de información financiera que le es aplicable, procurando una visión independiente de la entidad.

Para ello, la institución debe asegurar que el auditor externo:

23.1 Designa un equipo de Auditoría conformado por un número adecuado de personas competentes y con experiencia para la función, con conocimiento del negocio y en particular en métodos y técnicas actuariales para revisar la metodología y los cálculos implícitos en las reservas técnicas.

23.2 Comprende su responsabilidad hacia la institución y todas las partes interesadas.

23.3 Actúa con objetividad e independencia en la planificación de las actividades y en la ejecución de la auditoría.

23.4 Reporta todos los hallazgos significativos y conclusiones de su trabajo tanto a la Dirección como al Supervisor.

ESTÁNDARES DE GESTIÓN DE RIESGOS (R)

EL SISTEMA DE GESTIÓN DE RIESGOS

Una competencia clave de las empresas aseguradoras es su capacidad de gestionar los riesgos que asume en forma prudente y rentable.

La empresa aseguradora debe por lo tanto implementar un Sistema de Gestión de Riesgos, definido como el conjunto de políticas, procedimientos y mecanismos de control para propiciar una apropiada identificación, medición, control y monitoreo de los riesgos a los que se encuentra expuesta.

RIESGO DE SEGURO

El riesgo de seguro se define como la posibilidad de que la entidad vea afectado su patrimonio debido a la modificación adversa del valor de los compromisos asumidos en virtud de los seguros, debido a la inadecuación de las hipótesis de tarificación y constitución de reservas técnicas.

El riesgo de seguro surge como consecuencia de políticas y prácticas inadecuadas en el diseño de productos, la suscripción y la estimación del pasivo debido a errores en las hipótesis asumidas para la constitución de reservas técnicas.

Las políticas comprenden las políticas de suscripción de riesgos, constitución de reservas técnicas y reaseguro de la Institución.

El reaseguro y el coaseguro (especialmente en seguros generales) permiten mitigar este riesgo transfiriéndolo a compañías de reaseguro o compartiéndolo con otras entidades aseguradoras. Por su parte, el reaseguro constituye una fuente potencial de riesgo asociada a errores en el diseño y la administración del programa de reaseguro.

24. El Directorio debe aprobar la estrategia y las políticas para la gestión del riesgo de seguros y revisarlas periódicamente. La estrategia debe contemplar el apetito de riesgo y el perfil de riesgos de la institución. El Directorio debe revisar regularmente las exposiciones al riesgo de seguros y asegurar que los niveles de riesgos se encuentran dentro del marco establecido.

Para ello el Directorio debe:

24.1 Aprobar y mantener actualizada la estrategia y políticas de gestión del riesgo de seguros. Estas políticas deben ser consistentes con el apetito de riesgo definido y ser divulgadas eficazmente a toda la institución.

24.2 Las políticas referidas al riesgo de seguro deben:

- Ser consistentes con la naturaleza, volumen y complejidad del negocio.
- Estar detalladas por rama, producto o línea de negocio e incluir límites de exposición.
- Establecer los niveles de aprobación.
- Establecer el régimen de excepciones y nivel de aprobación para las mismas.
- Ser revisadas periódicamente.

24.3 Las políticas de suscripción deben:

- Considerar los riesgos asegurables y las coberturas que la compañía mantendrá cautela o directamente no asumirá.
- Establecer límites de concentración relevantes por ejemplo por rama, región geográfica, producto, industria, grupo, características de salud específicas u otro perfil de riesgo.

24.4 Las políticas de constitución de reservas técnicas deben:

- Estar basadas en estándares actuariales internacionales.
- Considerar la experiencia siniestral de la institución.
- Considerar la constitución de reservas adicionales en caso de no ser suficientes.

24.5 El programa de reaseguro debe considerar[4]:

- Los objetivos de la estrategia de reaseguro y establecer los parámetros bajo los cuales esta estrategia será controlada.
- La definición de los tipos de reaseguro apropiados para las distintas coberturas que comercializa considerando la capacidad técnica y financiera de la entidad.
- La posición respecto al uso de financiamiento a través de reaseguro financiero y fronting.

24.6 Evaluar periódicamente los resultados por rama y por producto de la institución y en función de los mismos evaluar cambios en la estrategia, políticas de riesgo y apetito de riesgo.

24.7 Revisar periódicamente la efectividad de la gestión del riesgo de seguro, mediante estudios de exposición a los riesgos, adecuación técnica de las tarifas, adecuación de las reservas y de los reaseguros contratados.

24.8 Identificar líneas de responsabilidad y autoridad en la gestión del riesgo de seguros.

24.9 Asegurar la realización de revisiones independientes para que en forma periódica se validen los procesos, las políticas, los procedimientos y que se instrumenten las acciones apropiadas ante las debilidades o fallas significativas detectadas por el auditor interno, externo, supervisor o profesional independiente que se expida sobre el trabajo realizado por la función actuarial.

24.10 Asegurar que la Alta Gerencia implemente las políticas y los procesos necesarios para que los riesgos asumidos sean consistentes con la estrategia, políticas y procedimientos aprobados.

[4] Los estándares relacionados a la selección de los reaseguradores se incluyen dentro de riesgo de crédito.

25. La Alta Gerencia debe implementar la estrategia y las políticas aprobadas por el Directorio para el riesgo de seguros y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe:

25.1 Implementar procesos acordes con la estrategia y la política definida por el Directorio que permitan una suscripción adecuada de los riesgos, la valoración adecuada de las reservas y el cumplimiento del programa de reaseguro.

25.2 Informar al Directorio sobre la exposición de la entidad a las distintas fuentes de riesgo de seguros.

25.3 Asegurar que las personas involucradas en el proceso de gestión de este riesgo tienen las capacidades, conocimientos y herramientas para cumplir con sus responsabilidades, incluyendo la evaluación de la suficiencia de los recursos y la capacitación de agentes y corredores de seguros.

25.4 Autorizar las notas técnicas de los nuevos productos de seguros, considerando las bases técnicas utilizadas y el cumplimiento de las disposiciones normativas establecidas al respecto.

25.5 Revisar periódicamente la estrategia, las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

26. La institución debe contar con una función actuarial profesional y permanente que participe en la definición de las políticas y procedimientos del riesgo de seguros y en la valuación de las reservas técnicas.

Para ello la función actuarial debe:

26.1 Contar con la capacidad, calificación y experiencia necesarias para la identificación del riesgo de seguros y su control. Quien desempeñe la función deberá tener conocimientos suficientes de matemática actuarial y financiera acordes con la naturaleza, el volumen y la complejidad de los riesgos asumidos. Asimismo debe contar con los recursos necesarios para cumplir su función adecuadamente.

26.2 Ser desarrollada en forma objetiva, imparcial e independiente del área comercial, ya sea por personal propio o contratado.

26.3 Evaluar y brindar asesoría, al menos, en lo relativo a reservas técnicas, determinación de primas y fijación de precios, diseño y actualización de productos, así como al cumplimiento de requisitos legales y regulatorios relacionados. Comprende, como mínimo, la evaluación y asesoría de los siguientes aspectos:

- El riesgo de seguro de la empresa.
- Las políticas de suscripción, reservas, reaseguros y fijación de precios.
- La posición de solvencia de la empresa, que incluya la solvencia futura y el cálculo de capital mínimo requerido a efectos regulatorios.
- Los contratos de reaseguro.
- El desarrollo y diseño de los productos que incluya la actualización de pólizas y notas técnicas de acuerdo a la normativa.
- Los procedimientos para el cálculo de reservas técnicas, incluidas la suficiencia y adecuación, integridad y exactitud de los datos utilizados.

27. La institución cuenta con una adecuada clasificación de riesgos asegurables y tarificación.

Para ello, la institución debe:

27.1 Efectuar la clasificación de riesgos y tarificación con base en las políticas de suscripción, manuales de suscripción y notas técnicas definidas y considerar todos los aspectos relevantes en cada rama, producto o línea de negocio.

27.2 Poseer manuales de suscripción por ramas o por productos, los cuales estén sujetos a revisión periódica.

27.3 Contar con permisos/licencias de suscripción definidas, en las cuales se establezcan límites cualitativos y cuantitativos.

27.4 Realizar la fijación de las tarifas en base a criterios técnicos, teniendo en cuenta -cuando sea posible- la experiencia siniestral de la institución.

27.5 Documentar y resguardar el correcto empleo del material de suscripción que se utiliza (solicitudes, informes de inspección, pólizas, formularios de denuncias).

27.6 Aplicar con una frecuencia adecuada métodos de revisión y ajuste de tarifas u otras medidas monitoreando cambios en los precios y en la siniestralidad, de forma de evitar resultados técnicos negativos recurrentes o escenarios extremos por cambios en mortalidad, morbilidad, tasas y pérdidas máximas de exposición que puedan determinar que las primas resulten insuficientes para enfrentar los riesgos retenidos, es decir, después de la cobertura de reaseguro.

28. La Institución debe definir procedimientos para asegurar que las reservas técnicas representan adecuadamente los pasivos asumidos más allá de los requisitos regulatorios.

Para ello la Institución debe:

28.1 Garantizar la adecuación, integridad y exactitud de los datos utilizados en el cálculo de las reservas técnicas.

28.2 Asegurar la adecuación de las metodologías y modelos de base utilizados, así como las hipótesis utilizadas en los cálculos de las reservas técnicas.

28.3 Resguardar las conclusiones de su trabajo y la documentación respaldatoria de los cálculos realizados para su acceso por parte del Supervisor.

28.4 Revisar periódicamente dichos procedimientos.

29. La institución debe contar con un proceso adecuado para la gestión de siniestros.

La institución debe:

29.1 Contar con procedimientos adecuados para la gestión de los siniestros, que establezcan los criterios de apertura, liquidación y cierre, así como los criterios para acuerdos transaccionales.

29.2 Asegurar que la documentación de los legajos de siniestros y el sistema de archivo contenga toda la información relevante, que permita verificar la adecuada valuación de la reserva de siniestros pendientes, siendo deseable que los mismos se encuentren en formato digital.

30. La institución debe desarrollar procedimientos para asegurar que los contratos de reaseguro son apropiadamente suscritos.

Para ello la Institución debe asegurar que los reaseguros contratados:

30.1 Son consistentes con el programa de reaseguro y con la estrategia y exposición al riesgo definidas por el Directorio.

30.2 Son adecuadamente suscritos de forma de garantizar que es posible beneficiarse de los derechos adquiridos bajo los mismos.

31. La institución debe establecer y realizar controles para asegurar que las excepciones en las políticas, los procedimientos y límites son identificadas y reportadas oportunamente al nivel jerárquico apropiado.

Para ello, la institución debe:

31.1 Contar con mecanismos de control interno que aseguren que la gestión del riesgo de seguros se realiza de acuerdo con las políticas y procedimientos definidos por el Directorio y Alta Gerencia.

31.2 Establecer procedimientos de identificación, monitoreo, documentación y notificación de excepciones a las políticas y límites establecidos.

31.3 Asegurar que las posiciones que exceden niveles predefinidos reciban la atención de la Alta Gerencia en forma oportuna.

32. La institución cuenta con un sistema adecuado para la medición, monitoreo y control del riesgo de seguro.

Para ello la institución debe:

32.1 Medir la exposición al riesgo de seguro (insuficiencia de primas, valuación de reservas técnicas y adecuación del programa de reaseguro) y el impacto que su realización ocasionaría en los resultados y el patrimonio de la entidad.

32.2 Desarrollar un sistema de información que permita una oportuna y correcta agregación y notificación al Directorio y la Alta Gerencia de las exposiciones al riesgo de seguros, así como que permita evaluar la efectividad de la gestión del riesgo y cumplir con su rol de supervisión.

RIESGO DE CRÉDITO

El riesgo de crédito se define como la posibilidad de que la entidad vea afectado su patrimonio debido a la incapacidad de los deudores o las contrapartes de cumplir con los términos originalmente pactados.

33. El Directorio debe aprobar las políticas para la contratación de reaseguros y la colocación de sus activos en Instituciones Financieras.

Para ello el Directorio debe:

33.1 Aprobar las políticas respecto al riesgo de crédito, las que deben:

- Considerar la selección de empresas reaseguradoras con una calificación crediticia igual o superior a la establecida en la regulación.
- Considerar la selección de los intermediarios de reaseguros.
- Establecer la tolerancia al riesgo de crédito en las colocaciones en las Instituciones Financieras.
- Ser revisadas periódicamente

33.2 Establecer límites a nivel de contrapartes individuales y de contrapartes relacionadas entre sí (conjuntos económicos). Asignar facultades de aprobación, las que deberán ser consistentes con la capacidad y experiencia de los designados.

33.3 Estar permanentemente informado de las contrapartes relevantes con dificultades o potencialmente problemáticas.

33.4 Promover la aplicación de principios contables que reflejen las condiciones de deterioro.

33.5 Asegurar que la Alta Gerencia implementa procedimientos adecuados para que los riesgos asumidos sean consistentes con las políticas aprobadas y el riesgo se mantiene dentro de los límites establecidos.

34. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio para el riesgo de crédito y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe asegurar que:

34.1 Las actividades de la Institución respecto a las contrapartes son consistentes con la política establecida, existen procedimientos escritos, implementados efectivamente y las responsabilidades de aprobación y revisión de contrapartes se asignan clara y adecuadamente.

34.2 La contratación de reaseguros debe estar sujeta a la política establecida y ser transparente. Los criterios establecidos no deberían ser modificados en función de las características de las operaciones o de las empresas relacionadas.

34.3 Las personas involucradas en el proceso de identificación, medición y control de los riesgos de crédito tienen las capacidades, conocimientos y herramientas para cumplir con sus responsabilidades.

34.4 Existen procedimientos para identificar las contrapartes con dificultades y las potencialmente problemáticas (alerta temprana).

34.5 Se monitorean las exposiciones actuales frente a los límites fijados y se tienen procedimientos para incrementar el monitoreo y tomar medidas adecuadas si se acercan a los límites.

34.6 Las previsiones cumplen con la normativa y son adecuadas con el nivel de riesgo asumido, donde se monitorea permanentemente la situación de las contrapartes.

34.7 Se identifican las situaciones en las que se deba clasificar un grupo de contrapartes (en especial los reaseguradores) como relacionadas entre sí (conjunto económico) y por ende, como un solo riesgo.

35. La Institución debe implementar un sistema para administrar el riesgo de crédito. El sistema debe ser coherente con la naturaleza, el tamaño y la complejidad de la institución.

Para ello la Institución debe:

35.1 Contar con un sistema de medición de riesgo de crédito que incorpore las exposiciones con las contrapartes y que capture toda fuente material de riesgo.

35.2 Desarrollar un sistema de información que permita:

- Suministrar información sobre todas las exposiciones con contrapartes.
- Comparar las mediciones y exposiciones contra los límites de riesgo establecidos e informar sobre las excepciones a los mismos de manera oportuna y adecuada.
- Detectar concentraciones de riesgo.

35.3 Implementar procedimientos para:

- Identificar contrapartes con deterioro actual o potencial de manera temprana.
- El manejo de posiciones con contrapartes con problemas.

36. La institución debe realizar controles para asegurar que las excepciones en las políticas, los procedimientos y límites son reportadas oportunamente al Directorio y la Alta Gerencia.

36.1 Para ello la institución debe contar con mecanismos que aseguren que las excepciones sean reportadas rápidamente, estén claramente documentadas

y reciban la atención de la Alta Gerencia en forma oportuna. Debe existir una política explícita para la autorización de excepciones y sobre las acciones a tomar en dichos casos.

RIESGOS DE MERCADO

El riesgo de mercado se define como la posibilidad de sufrir pérdidas en posiciones dentro y fuera de balance debido a movimientos adversos de las variables de mercado. Se identifican como riesgos de mercado:

- Riesgo de tasa de interés
- Riesgo de tipo de cambio
- Riesgo de reajuste
- Otros riesgos de mercado

a. RIESGO DE TASA DE INTERÉS

El riesgo tasa de interés está integrado por los siguientes riesgos:

- Riesgo de tasa de interés del portafolio de inversiones – Es el riesgo asociado a las eventuales pérdidas en el valor de mercado del portafolio de inversiones originadas por movimientos adversos en las tasas de interés. Este riesgo tiene dos componentes:

**** Riesgo Específico: Deriva de movimientos adversos en el valor de mercado del portafolio de inversiones, originados en factores relacionados con los emisores de los instrumentos.***

**** Riesgo General: Proviene de movimientos adversos de precios originados por variaciones en las tasas de interés de mercado libres de riesgo.***

- Riesgo de tasa de interés estructural – Este riesgo abarca a todo el balance, incluyendo las posiciones fuera de balance. Es el riesgo potencial de que los resultados o el patrimonio de la entidad se vean afectados como consecuencia de movimientos en las tasas de interés. Este riesgo surge por la diferencia que existe entre el momento en que se modifican las tasas de los activos y de los pasivos de la entidad.

b. RIESGO DE TIPO DE CAMBIO

El riesgo tipo de cambio se define como la posibilidad de que el patrimonio se vea adversamente afectado por movimientos desfavorables en las tasas de cambio entre divisas para posiciones dentro y fuera de balance.

c. RIESGO DE REAJUSTE

El <u>riesgo de reajuste</u> es el riesgo de que el patrimonio se vea adversamente afectado por movimientos en los tipos de cambio de las unidades de cuenta en moneda nacional en un horizonte de largo plazo.

d. OTROS RIESGOS DE MERCADO

Los <u>otros riesgos de mercado</u> se definen como la posibilidad de que el patrimonio se vea afectado por movimientos adversos en el precio de acciones, precio de mercancías, precio de bienes raíces y/u otros activos de la economía real asociados a rendimientos de instrumentos financieros.

37. El Directorio debe aprobar la estrategia y las políticas para la gestión de los riesgos de mercado, las que deben reflejar el apetito de riesgo de la institución.

Para ello el Directorio debe:

37.1 Aprobar las políticas que influyen sobre el nivel de riesgo de mercado asumido por la institución. Estas políticas deben:

- ser consistentes con la naturaleza, volumen y complejidad de las actividades,
- definir los tipos, niveles y límites de riesgos aceptables, así como los parámetros cuantitativos para la aprobación de inversiones establecer el régimen de excepciones, el nivel de aprobación y la notificación de las mismas,
- ser revisadas periódicamente.

37.2 Identificar líneas de responsabilidad y autoridad en la gestión de los riesgos de mercado.

37.3 Recibir y revisar la información sobre los riesgos de mercado, la cual debe ser suficiente, detallada y oportuna, de forma que permita comprender los riesgos asumidos y evaluar el desempeño de la Alta Gerencia en el monitoreo y control de dichos riesgos.

37.4 Evaluar periódicamente que la política de inversiones implementada esté alineada con el apetito de riesgo y las políticas aprobadas.

37.5 Asegurar que la Alta Gerencia implementa las políticas y los procedimientos necesarios para que los riesgos asumidos sean consistentes con las políticas aprobadas y el riesgo se mantiene dentro de los límites establecidos.

37.6 Asegurar que la institución cuenta con una estructura organizacional adecuada para la gestión del riesgo de mercado.

38. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio para los riesgos de mercado y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe:

38.1 Implementar las políticas y procedimientos aprobados para gestionar los riesgos de mercado en el corto, mediano y largo plazo, de forma consistente con las políticas aprobadas.

38.2 Implementar un sistema de límites que asegure que las exposiciones a los riesgos se mantienen dentro de las políticas aprobadas por el Directorio.

38.3 Definir una metodología para valuar posiciones y medir el desempeño.

38.4 Desarrollar un sistema de información que le permita una oportuna y correcta agregación de las exposiciones al riesgo de mercado, así como evaluar la efectividad de la gestión del riesgo.

38.5 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

38.6. Asegurar que las personas involucradas en el proceso de identificación, medición y control de los riesgos de mercado tienen las capacidades, conocimientos y herramientas para cumplir con sus responsabilidades.

38.7 Asignar claramente las responsabilidades a quienes asumen posiciones de riesgos, funciones de medición y control, elaboración de reportes u otras áreas administrativas.

38.8 Asegurar que existan mecanismos efectivos de control y de corresponder implementar controles eficaces sobre los modelos utilizados para identificar y cuantificar el riesgo de mercado.

38.9 Contar con un proceso para analizar nuevos productos y actividades, que considere el riesgo de mercado en forma explícita.

39. La institución debe tener un sistema de medición de riesgo de mercado que capture toda fuente material de riesgo tasa de interés, tipo de cambio, reajuste y otros riesgos de mercado y evaluar el impacto de los mismos sobre la institución. Los supuestos subyacentes en dichos sistemas deben ser comprendidos claramente por el Directorio y la Alta Gerencia.

En general, el sistema debe:

39.1 Incorporar las exposiciones que provienen de todas las actividades de la institución.

39.2 Evaluar el impacto de los cambios en los resultados y el valor económico de la institución.

39.3 Identificar excesos en límites establecidos.

39.4 Utilizar conceptos financieros y técnicas de medición de riesgos de mercado generalmente aceptados.

39.5 Tener un grado de detalle y complejidad que sea consistente con el nivel de riesgo asumido.

39.6 Asegurar que los supuestos están claramente documentados y que pueden ser comprendidos por la Alta Gerencia. Dichos supuestos deben ser revisados por lo menos anualmente.

39.7 Realizar mediciones bajo condiciones de estrés y considerar los resultados en la definición del apetito al riesgo de la institución.

40. La institución debe tener un sistema adecuado para el monitoreo y control de los riesgos de mercado.

40.1 Para ello, el sistema de monitoreo y control debe:

- Controlar los límites y métricas aprobadas.
- Incluir procedimientos y metodologías de control claramente establecidas y definidas.
- Fijar límites globales para la institución y límites específicos para portafolios individuales, actividades o unidades de negocio.
- Ser consistente con la forma de medición de riesgos de la institución y ser revisado periódicamente.

41. La institución debe establecer y realizar controles para asegurar que las excepciones en las políticas, los procedimientos y los límites son identificados y reportados oportunamente al nivel jerárquico apropiado.

41.1 Establecer procedimientos de identificación, monitoreo, documentación y notificación de excepciones a las políticas y límites establecidos.

41.2 Asegurar que las posiciones que exceden los niveles predefinidos reciben la atención de la Alta Gerencia en forma oportuna. Las excepciones a los límites deben ser reportadas rápidamente a la Alta Gerencia.

42. La institución debe contar con un sistema de información gerencial que suministre información adecuada y oportuna sobre las exposiciones a los riesgos de mercado al Directorio y la Alta Gerencia.

Un sistema informativo, fiel y oportuno es esencial para gestionar las exposiciones de riesgos de mercado y asegurar el cumplimiento con las políticas establecidas por el Directorio.

Para ello, el sistema debe:

42.1 Emitir reportes en forma regular y comparar las exposiciones con los límites establecidos.

42.2 Incluir una comparación de las proyecciones con los resultados reales para permitir la identificación de limitaciones o errores en los modelos.

42.3 Prever que los reportes que emite sean revisados por el Directorio y la Alta Gerencia regularmente.

RIESGO DE LIQUIDEZ

El riesgo de liquidez es la posibilidad de que la entidad no cuente con suficientes activos líquidos para hacer frente a las obligaciones asumidas. Este riesgo comprende el riesgo de liquidez de mercado que proviene de la dificultades derivadas de los cambios en las condiciones de mercado que afecten la liquidación de los activos, ya sea en los tiempos de realización, como en el valor de venta obteniendo un valor inferior al de mercado para dichos activos.

43. El Directorio debe aprobar la política respecto a la gestión del riesgo de liquidez de la Institución.

Para ello, el Directorio debe:

43.1 Aprobar políticas vinculadas al manejo del riesgo de liquidez de la institución y revisarlas periódicamente.

43.2 Aprobar y revisar periódicamente los planes de contingencia de la Institución para enfrentar eventuales problemas de liquidez.

43.3 Asegurar que la institución cuenta con una estructura organizacional adecuada para la gestión del riesgo de liquidez.

43.4 Aprobar límites a las exposiciones al riesgo de liquidez y revisarlos regularmente.

43.5 Identificar líneas de responsabilidad y autoridad en la gestión del riesgo de liquidez.

43.6 Contar con información suficiente, detallada y oportuna sobre la gestión del riesgo de liquidez, realizar una revisión periódica sobre la efectividad de la gestión y del desempeño de la Alta Gerencia en el monitoreo y control de dicho riesgo.

43.7 Asegurar que la Alta Gerencia implementa procedimientos adecuados para que los riesgos asumidos sean consistentes con las políticas aprobadas.

44. La Alta Gerencia debe implementar las políticas aprobadas por Directorio para el riesgo de liquidez y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe:

44.1 Implementar las políticas y desarrollar procedimientos específicos para la gestión del riesgo de liquidez, que tengan en cuenta el marco definido de gestión de activos y pasivos, las condiciones establecidas en los contratos de reaseguro que afectan la liquidez, diferentes monedas, activos radicados en diferentes países y el uso de distintos instrumentos financieros.

44.2 Definir los responsables de la administración del riesgo de liquidez y el mecanismo a través del cual se implementa la política de liquidez y se revisan las decisiones tomadas sobre la posición de liquidez.

44.3 Implementar un sistema de límites para asegurar que la liquidez se mantiene dentro de las políticas aprobadas por el Directorio.

44.4 Asegurar que las personas involucradas en el proceso de identificación, medición y control del riesgo de liquidez tienen las capacidades, conocimientos y herramientas para cumplir con sus responsabilidades.

44.5 Desarrollar e implementar planes de contingencia para hacer frente a flujos de salida inesperados o problemas en el mercado de capitales que afecten la liquidez de las inversiones y dificulten el acceso a las fuentes alternativas de liquidez.

El plan de contingencia debe:

- Establecer procedimientos que aseguren que los flujos de información son oportunos e ininterrumpidos y que proporcionan a la Gerencia la información precisa para tomar decisiones rápidas.

- Incluir las acciones a tomar en el caso de enfrentarse con un problema de liquidez, como por ejemplo: el orden de prioridad de liquidación de activos en caso de ser necesario, o las fuentes de fondos alternativos.

45. La institución debe establecer un sistema de medición y monitoreo continuo de los requerimientos netos de fondos.

Para ello, el sistema debe:

45.1 Tener la capacidad de calcular las posiciones de liquidez (flujos de efectivo prospectivos) a corto y mediano plazo, en situaciones de estrés, por moneda y en forma agregada.

45.2 Ser lo suficientemente flexible como para enfrentar contingencias que puedan surgir.

45.3 Brindar información, en todo momento, de los niveles de activos líquidos mantenidos.

46. La institución debe establecer mecanismos de control que aseguren el cumplimiento de los límites de liquidez definidos y contar con un proceso adecuado para la identificación y tratamiento de las excepciones.

Para ello, la institución debe:

46.1 Contar con mecanismos de control interno que aseguren que el manejo del riesgo de liquidez se realiza de acuerdo con las políticas y procedimientos definidos por el Directorio y la Alta Gerencia.

46.2 Establecer procedimientos de identificación, monitoreo, documentación y notificación de excepciones a las políticas y límites establecidos.

46.3 Asegurar que las posiciones que exceden niveles predefinidos reciban la atención de la Alta Gerencia de forma oportuna.

47. La institución debe contar con sistemas de información adecuados para monitorear, controlar e informar el riesgo de liquidez. Los informes deben entregarse periódicamente al Directorio y Alta Gerencia.

Para ello, el sistema debe:

47.1 Emitir información en forma regular, que permita el control de exposiciones al riesgo de liquidez actuales en relación a los límites establecidos.

47.2 Permitir una evaluación del nivel y de las tendencias en la exposición agregada al riesgo de liquidez de la Institución.

RIESGO OPERACIONAL

El riesgo operacional se define como el riesgo presente y futuro de que las ganancias o el patrimonio de la entidad se vea afectado por pérdidas resultantes de procesos, personal o sistemas internos inadecuados o defectuosos, o por eventos externos.

Incluye además el riesgo de cumplimiento, es decir, la posibilidad de que una entidad se vea afectada por violaciones a las leyes, regulaciones, estándares y prácticas de la industria o estándares éticos. Este riesgo también aparece en situaciones en donde las leyes o regulaciones que rigen ciertos productos o actividades son ambiguas.

El riesgo operacional acompaña el desarrollo y evolución de los productos, el desarrollo e implementación de los sistemas, los procesos transaccionales y guarda relación con la calidad del personal y el ambiente de control interno. Es un riesgo diferente a otros, como el riesgo de crédito o de mercado, ya que no se asume riesgo operacional con el objetivo de obtener un retorno, sino que surge de la actividad normal de la entidad y afecta el manejo integral de riesgos.

La entidad puede tener su propia definición del riesgo operacional, pero cualquiera sea ésta, es crítico que exista una comprensión del concepto por parte de la entidad para su manejo efectivo.

Cada entidad puede tener una forma de organización diferente para esta función de acuerdo con su tamaño, complejidad y líneas de negocio. Sin perjuicio de ello, la institución debe asignar los recursos necesarios, definir claramente responsabilidades, tener independencia operativa para el ejercicio de la función y estar sujeta a revisiones periódicas por parte de la Auditoría interna.

La resiliencia operativa es la capacidad de mantener operaciones críticas en caso de interrupciones. Adoptar un enfoque de resiliencia operativa permite a las instituciones identificar y protegerse de amenazas y posibles fallas, responder y adaptarse, así como recuperarse y aprender de eventos disruptivos para minimizar su impacto en la entrega de operaciones críticas, teniendo en cuenta su apetito de riesgo.

A la hora de definir e implementar el enfoque de resiliencia, deben tenerse en cuenta aspectos vinculados a gobernanza, gestión de riesgo operacional, planificación y pruebas de continuidad del negocio, interdependencia de operaciones críticas y los procesos y sistemas que las soportan, dependencia de terceros, administración de incidentes, tecnología de la información y comunicaciones y ciberseguridad.

48. El Directorio debe aprobar los principios generales para el manejo del riesgo operacional, el apetito del riesgo y las políticas de la institución, y revisarlos periódicamente. Asimismo, debe revisar regularmente la exposición al riesgo operacional y asegurar que los niveles de riesgos se encuentran dentro del marco establecido.

Para ello, el Directorio debe:

48.1 Aprobar las políticas en relación al riesgo operacional y revisarlas periódicamente. Estas políticas deben ser consistentes con el apetito de riego definido.

Las mismas deben:

- Reconocer el riesgo operacional (el cual incluye el riesgo de cumplimiento) como un riesgo que la entidad debe manejar explícitamente.
- Constituir una guía clara en relación al control de este riesgo y asegurar que todo el personal está comprometido con dichas actividades de control.

48.2 Promover una cultura de control adecuada en la organización y el cumplimiento de las leyes, regulaciones, prácticas de la industria y estándares éticos.

48.3 Asegurar que la gestión del riesgo operacional se lleva a cabo en forma continua.

48.4 Revisar periódicamente la efectividad de la gestión del riesgo operacional.

48.5 Asegurar que se cuenta con una estructura organizacional adecuada para la gestión del riesgo operacional.

48.6 Identificar líneas de responsabilidad y autoridad en la gestión del riesgo operacional.

48.7 Aprobar los lineamientos estratégicos del enfoque de resiliencia operativa de manera consistente con el apetito de riesgo.

48.8 Aprobar las políticas en relación a Seguridad de la Información y revisar periódicamente la efectividad de su implementación.

Las mismas deben:

- Reconocer explícitamente los riesgos vinculados a la gestión de activos de información y la necesidad de que su gestión sea consistente con la naturaleza y el nivel de complejidad de las operaciones.
- Constituir una guía clara en relación a la gestión de seguridad de la información.
- Promover una adecuada cultura de seguridad de la información.

48.9 Contar con información suficiente, detallada y oportuna sobre el riesgo operacional de forma que le permita comprender los riesgos asumidos y evaluar el desempeño de la Alta Gerencia en el monitoreo y control de dicho riesgo.

48.10 Asegurar la realización de revisiones independientes para que en forma periódica se validen los procesos, las políticas, los procedimientos. Asegurar que se instrumenten las acciones apropiadas ante las debilidades o fallas significativas detectadas por el auditor interno, externo, supervisor o profesional independiente.

48.11 Asegurar que la Alta Gerencia implemente las políticas y los procesos necesarios para que los riesgos asumidos sean consistentes con las políticas aprobadas.

49. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio en relación al riesgo operacional y desarrollar procedimientos apropiados para su identificación, medición, monitoreo y control. Estas políticas y procedimientos deben considerar el riesgo operacional en todas las actividades de la institución.

Para ello, la Alta Gerencia debe:

49.1 Implementar las políticas y desarrollar procedimientos para gestionar el riesgo operacional, de forma consistente con las políticas definidas.

49.2 Implementar un modelo de tres líneas de defensa acorde a la naturaleza, volumen y complejidad de las operaciones y de su nivel y tipología de riesgos operacionales.

49.3 Asignar responsabilidades en forma explícita para el manejo del riesgo operacional, independientemente de la estructura organizacional que se defina. En particular, se asignan y definen roles y responsabilidades sobre la seguridad de la información.

49.4 Asignar los recursos necesarios en cantidad, calidad y competencia a efectos de un buen manejo del riesgo operacional.

49.5 Identificar adecuadamente las fuentes potenciales de riesgo operacional y en consecuencia establecer mecanismos que mitigan este riesgo.

49.6 Establecer que la función de seguridad de la información debe ser independiente funcional y presupuestalmente del área de TI.

49.7 Asegurar que en el proceso de creación de nuevos productos o en la revisión de procesos, se considera el riesgo operacional en forma explícita.

49.8 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

49.9 Desarrollar un sistema de información que permita una oportuna y correcta notificación al Directorio del riesgo operacional así como que permita evaluar la efectividad de gestión del riesgo.

50. La Alta Gerencia debe implementar las políticas y desarrollar procedimientos apropiados para la identificación, medición, monitoreo y control del riesgo de cumplimiento y reportar al Directorio sobre el manejo de este riesgo.

Para ello, la Alta Gerencia debe:

50.1 Asignar responsabilidades en forma explícita para el manejo del riesgo de cumplimiento, independientemente de la estructura organizacional que se defina.

50.2 Identificar adecuadamente las fuentes potenciales de riesgo de cumplimiento, y en consecuencia establecer mecanismos que mitigan este riesgo.

50.3 Asegurar que el Directorio reciba en forma periódica información sobre la efectividad de la función de cumplimiento y en particular, cualquier aspecto que represente un riesgo de cumplimiento significativo.

50.4 Asegurar que exista un proceso que asegure el cumplimiento con las leyes y las regulaciones bancocentralistas.

50.5 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

50.6 Desarrollar un sistema de información que permita una oportuna y correcta agregación y notificación al Directorio del riesgo operacional y de cumplimiento así como que permita evaluar la efectividad de su gestión.

51. La institución debe contar con procedimientos de identificación, medición y evaluación de las fuentes de riesgo operacional y definir los mecanismos para mitigar dichos riesgos.

Para ello, la institución debe:

51.1 Realizar un mapeo de los distintos procesos y revisarlo periódicamente.

51.2 Establecer algún mecanismo de autoevaluación de riesgos a nivel de los distintos procesos operativos de la entidad y definir controles orientados a mitigar dichos riesgos.

51.3 Involucrar al personal vinculado a los distintos procesos en este mecanismo de auto evaluación.

51.4 Generar un sistema de indicadores que alerten sobre debilidades en los procesos.

51.5 Llevar un registro de los eventos de riesgo operacional que permita su consolidación y análisis.

51.6 Llevar un registro de las incidencias generadas en el proceso de atención a los clientes.

51.7 Realizar análisis de escenarios, incluidos eventos de baja probabilidad y alto impacto, algunos de los cuales podrían resultar en pérdidas graves por riesgo operativo y afectar la resiliencia operativa.

51.8 Contar con procedimientos que permitan asegurar el cumplimiento con las leyes, normas e instrucciones emitidas por entes reguladores..

51.9 Analizar integralmente los resultados de las diferentes herramientas de medición y gestión de riesgos implementadas en la institución así como en la industria, para mejorar la comprensión del perfil de riesgo operativo y la toma de decisiones.

51.10 Informar los resultados de las distintas herramientas de gestión de riesgo operacional a la Auditoría Interna y al Comité de Auditoría y comunicarlas al personal involucrado.

52. La institución debe implementar procedimientos de control y monitoreo del riesgo operacional.

Para ello la institución debe:

52.1 Asegurar que exista un estrecho contacto entre las estructuras de control y se intercambie información sobre el resultado de las actuaciones de cada una de ellas.

52.2 Asegurar que los procesos (o partes de ellos) que se encuentren tercerizados están adecuadamente controlados.

52.3 Asegurar que existan reportes periódicos al Directorio sobre la eficacia de las políticas implementadas. La frecuencia y profundidad de los reportes dependerá del nivel de riesgos y los cambios en el perfil y deberán tener un enfoque proactivo.

53. El área o responsable de TI debe proporcionar los servicios en un ambiente seguro, que incluya no solamente las condiciones operativas de esta área sino también factores tales como confiabilidad, confidencialidad, integridad y disponibilidad. Incluye además el soporte y la capacitación a los usuarios del servicio y la habilidad para manejar problemas e incidentes, operaciones, desempeño del sistema, planificación de la capacidad y administración de los datos e instalaciones.

Las prácticas de manejo de riesgos promoverán operaciones de TI efectivas, seguras y sólidas, que aseguren la continuidad de las operaciones y la confiabilidad y disponibilidad de la información. El manejo del riesgo operacional derivado de los sistemas debe comprender a toda la organización y proveedores externos.

Debe asegurarse que se cumplan con los siguientes requerimientos:

53.1 Proporcionar un nivel de servicio que satisfaga las necesidades del negocio.

53.2 Establecer controles adecuados de los datos a nivel de la operación, entradas, proceso y salidas.

53.3 Asegurar la calidad de los procesos y/o los programas que monitorean la capacidad y el desempeño del servicio de TI.

53.4 Asegurar la calidad de la asistencia proporcionada a los usuarios, incluida la habilidad para manejar problemas.

53.5 Contar con adecuadas políticas operativas, procedimientos y manuales.

53.6 Generar y mantener actualizado el (los) inventario de dispositivos físicos, sistemas, aplicaciones y plataformas de software utilizados en la organización, incluyendo actividades periódicas de control interno para su verificación.

53.7 Gestionar los activos de TI a través de su ciclo de vida para asegurar que continúan operativos en condiciones acordes a los niveles de servicio establecidos, y que la finalización de uso es gestionada adecuadamente.

53.8 En el caso de servicios prestados por terceros, debe asegurar que:

- Se han documentado adecuadamente a través de contratos, las condiciones y niveles mínimos de servicio a ser obtenidos del proveedor.
- Se han establecido controles adecuados sobre los proveedores externos y que la institución es capaz de monitorear los mismos.
- El servicio a los requerimientos de los usuarios es adecuado.
- El proveedor es capaz de proveer y mantener el desempeño de los niveles de servicios adecuado a las necesidades de los usuarios.

54. La institución debe contar con un plan de contingencia y de continuidad de los negocios que permita operar ante la ocurrencia de eventos externos severos y se enmarque en el enfoque de resiliencia operativa adoptado.

Para ello la institución debe:

54.1 Contar con un Análisis de Impacto al Negocio con el cual se identifiquen las actividades críticas de la institución.

54.2 Establecer planes que ante distintos escenarios de desastre, aseguren la continuidad del negocio. Los mismos deben diseñarse para permitir la recuperación de las operaciones y para no interrumpir el servicio prestado por los centros de procesamiento de datos, redes, proveedores externos y unidades de negocios.

54.3 Abarcar en sus planes la continuidad de los servicios tercerizados.

54.4 Establecer planes de respaldo de información que aseguren su recuperabilidad.

54.5 Revisar periódicamente la aplicabilidad de estos planes. Para esto, se debe realizar una prueba (parcial o completa) del plan por lo menos anualmente, debidamente documentada y analizada al culminarse.

55. La institución debe contar con una gestión integral e independiente de la Seguridad de la Información.

Para ello la institución debe:

55.1 Mantener actualizado el inventario y la clasificación de sus activos de información, debiendo asignarse dueño y custodio en todos los casos.

55.2 Implementar estándares, procedimientos y directrices que permitan preservar la confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta aspectos de seguridad física y lógica.

55.3 Definir una política de control de acceso que incorpore los principios de menor privilegio y segregación de funciones. Definir y establecer los niveles, controles y trazas necesarias y asegurar el cumplimiento de las mismas

55.4 Identificar, evaluar, tratar y monitorear los riesgos asociados a la gestión de sus activos de información, de manera que se incluya un análisis sobre las amenazas y vulnerabilidades presentes.

55.5 Contar con indicadores y medidas que contribuyan al monitoreo de la gestión de la seguridad de la información.

55.6 Generar concientización y asegurar una adecuada capacitación al personal que permita involucrar a todos en la gestión de los riesgos asociados a los activos de información.

55.7 Generar instancias de sensibilización a los clientes en materia de seguridad de la información, educando sobre los riesgos asociados al uso de los distintos canales y promoviendo las mejores prácticas.

55.8 Asegurar el cumplimiento de las políticas de seguridad de la información en el caso de actividades tercerizadas y velar por la seguridad de los datos procesados externamente.

55.9 Contar con una política, procedimientos e indicadores de gestión de incidentes de seguridad y llevar a cabo pruebas frecuentemente de manera de tener actualizados las actividades a realizar.

56. La función de cumplimiento debe contar con mecanismos para identificar, medir, controlar y monitorear el riesgo de cumplimiento asumido.

Para ello la función de cumplimiento debe:

56.1 Asesorar al Directorio y a la Alta Gerencia del cumplimiento de las leyes, normativas y estándares aplicables por parte de la institución.

56.2 Contar con la suficiente autoridad, importancia, independencia, recursos y acceso al Directorio.

56.3 Promover y participar activamente en la capacitación de todos los funcionarios en materia de cumplimiento, actuar de punto de contacto para preguntas sobre cumplimiento y guiar sobre la aplicación adecuada de las leyes, normas, estándares aplicables, políticas y procedimientos, códigos de ética y de buenas prácticas.

56.4 Implementar mecanismos para identificar y evaluar el riesgo de cumplimiento existente en las distintas actividades de la entidad, incluyendo los productos nuevos, las propuestas de nuevos tipos de negocios o cualquier cambio en las características del relacionamiento con los clientes.

56.5 Establecer mecanismos para medir el riesgo de cumplimiento y usar estas medidas para mejorar el manejo de este riesgo. Algunos indicadores pueden ser utilizados con el apoyo tecnológico respectivo, para identificar y medir potenciales problemas de cumplimiento.

56.6 Implementar mecanismos para monitorear la efectividad de las políticas mediante pruebas sobre el cumplimiento.

56.7 Reportar al Directorio sobre los resultados del monitoreo y en general, sobre el perfil general del riesgo de cumplimiento basado en los indicadores definidos.

57. La información suministrada al supervisor debe ser confiable y oportuna y debe existir un responsable en la organización por su elaboración y presentación.

La información suministrada por la entidad es un insumo básico para que el supervisor pueda cumplir con sus responsabilidades. Por tanto, la calidad de dicha información es fundamental y constituye un elemento esencial en la definición del alcance de las actividades que debe desarrollar.

Los sistemas de contabilidad y procedimientos utilizados son un elemento crítico en la evaluación del perfil de riesgos de una institución y de su condición financiera y patrimonial.

Para que el proceso de generación de información al supervisor sea confiable debe:

57.1 Tener políticas y procedimientos claros sobre el tratamiento contable consistente con los requisitos regulatorios y los estándares internacionales.

57.2 Asegurar que los procesos de contabilización son eficaces y controlados, evitando el diferimiento en la contabilización de las operaciones.

57.3 Contar con un proceso automatizado de generación de información, donde ésta fluya naturalmente desde las transacciones a los productos finales de información.

57.4 Estar dotado de un sistema de controles adecuados (separación de funciones, actividades de control, reportes, etc.).

57.5 Contar con recursos suficientes y capacitados para llevar adelante la tarea en tiempo y forma.

57.6 Estar sometido a revisiones independientes periódicas por parte de la Auditoría Interna.

57.7 Contar con un responsable por la generación de información hacia el exterior de la empresa (tanto para el supervisor como para cualquier usuario externo).

58. La institución debe establecer mecanismos de revisión independiente y periódica del proceso de gestión del riesgo operacional. Los resultados de las revisiones deben ser reportados directamente al Directorio y a la Alta Gerencia.

La revisión independiente debe incluir la evaluación de:

58.1 El sistema en su conjunto y su eficacia en el cumplimiento de los objetivos.

58.2 El cumplimiento efectivo de las políticas y procedimientos y la adecuada documentación de los procesos y las decisiones adoptadas.

58.3 La organización y la suficiencia de los recursos humanos en cuanto a número y competencia técnica para gestionar en forma correcta el riesgo.

58.4 La capacidad y eficacia del sistema para capturar todos los elementos materiales de riesgo.

58.5 La confiabilidad y corrección en el procesamiento, agregación y cotejo de los datos.

58.6 Los cambios significativos que puedan afectar la efectividad de los controles, como cambios en los mercados, recursos humanos, tecnología o estructuras de cumplimiento.

58.7 La calidad de las revisiones y si son llevadas a cabo por individuos independientes de las áreas sujetas a revisión y con la formación y experiencia suficientes y si existe un proceso de seguimiento y corrección de hallazgos significativos por parte de la Alta Dirección y el Directorio.

RIESGO DE LAVADO DE ACTIVOS, FINANCIAMIENTO DEL TERRORISMO Y PRODUCCIÓN DE ARMAS DE DESTRUCCION MASIVA (LA/FT/PADM) [5]

El riesgo de LA/FT/PADM refiere a la posibilidad de pérdida o daño que puede sufrir una entidad al ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas y/o producción de armas de destrucción masiva, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

Se considera que existe un mayor riesgo de LA/FT/PADM en los seguros de vida de prima única con rescate anticipado y en aquellos productos que habiliten diferentes formas de inversión.

Las instituciones deberán instrumentar un sistema que abarque políticas, prácticas y procedimientos que le permitan prevenirse de ser utilizada como instrumento para el lavado o la canalización de fondos destinados al financiamiento del terrorismo o a la producción de armas de destrucción masiva. Para ello, las instituciones deben contar con políticas y procedimientos bien documentados y correctamente comunicados a todo el personal pertinente, estar integradas en la gestión integral de riesgos de la institución y deben ser aplicados en forma continua.

[5] A partir de la sanción de la Ley 19.574 de 10.01.2018 artículo 12, el alcance del riesgo de LA/FT/PADM para las aseguradoras se restringió a seguros de vida y otros seguros relacionados con la inversión.

59. El Directorio debe aprobar las políticas que propicien una adecuada gestión del riesgo de LA/FT/PADM y revisarlas periódicamente.

Para ello, el Directorio debe:

59.1. Aprobar las políticas en relación al riesgo de LA/FT/PADM y revisarlas periódicamente.

Las mismas deben:

- Promover normas éticas y profesionales de alto nivel para impedir que la institución sea utilizada con fines delictivos.
- Definir criterios para la prevención y detección de actividades delictivas y la notificación de las actividades sospechosas al supervisor.
- Definir criterios claros de aceptación de inicio y cese de vinculación con clientes.
- Establecer criterios de selección, evaluación y capacitación del personal e intermediarios de seguros.
- Asegurar la privacidad en el manejo de información.

59.2 Asegurar que exista una estructura organizacional con una adecuada separación de funciones y asignación de responsabilidades para la prevención de este riesgo, que contemple la designación del Oficial de Cumplimiento con la preparación e idoneidad adecuada, asignándole jerarquía dentro de la organización así como los recursos humanos y materiales necesarios para desarrollar su tarea en forma autónoma y eficiente.

59.3 Conocer y entender los riesgos de LA/FT/PADM a los que se encuentra expuesta la entidad a efectos de definir políticas acorde a los riesgos identificados y evaluar el desempeño de la Alta Gerencia y en particular del Oficial de Cumplimiento, en el monitoreo y control de este riesgo.

59.4 Asegurar la realización de revisiones independientes para que en forma periódica se validen los procesos, las políticas, los procedimientos y los controles relativos al sistema de prevención de LA/FT/PADM. Asegurar que se instrumenten las acciones apropiadas ante las debilidades o fallas significativas detectadas por el auditor interno, externo, supervisor o profesional independiente.

60. La Alta Gerencia debe asegurar la implementación de las políticas aprobadas por el Directorio en relación al riesgo de LA/FT/PADM así como el desarrollo de procedimientos para la identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe:

60.1 Conocer y analizar periódicamente los riesgos a los que se encuentra expuesta la entidad considerando todos los factores relevantes para determinar su perfil de riesgo y el adecuado nivel de mitigación que se aplicará.

60.2 Instrumentar una estructura organizacional con clara definición de responsabilidades, que cuente con los recursos necesarios en cantidad, conocimiento técnico y experiencia, que aseguren un eficaz cumplimiento de las actividades de análisis, monitoreo y control del riesgo.

60.3 Implementar procedimientos para la administración de riesgo de LA/FT/PADM que permita identificar, medir, monitorear dicho riesgo, así como también reportar las operaciones sospechosas o inusuales y atender los requerimientos de información por parte de las autoridades competentes.

60.4 Asegurar que el personal comprenda su rol en el sistema de prevención y esté en conocimiento de los procedimientos y controles internos diseñados de forma de mitigar el riesgo de LA/FT/PADM.

60.5 Revisar periódicamente las políticas y procedimientos de forma de asegurar que continúan siendo adecuados, prudentes y acordes al nivel de riesgo de LA/FT/PADM de la actividad desarrollada.

60.6 Asegurar que en el proceso de creación de nuevos productos se considere el riesgo de LA/FT/PADM.

61. El Oficial de Cumplimiento es el responsable de la implantación, seguimiento y control del adecuado funcionamiento del sistema de prevención del riesgo de LA/FT/PADM.

Para ello, el Oficial de Cumplimiento, en su rol de encargado del sistema de prevención, debe:

61.1 Implementar las políticas aprobadas por el Directorio y desarrollar procedimientos bien documentados que permitan identificar, medir y controlar el riesgo de LA/FT/PADM, los cuales deben aplicarse en toda la institución y en los servicios tercerizados.

61.2 Proponer la actualización de políticas y procedimientos en relación al riesgo de LA/FT/PADM y el uso de herramientas adecuadas a la complejidad y el nivel de actividad de desarrollo.

61.3 Mantenerse actualizado y diseñar programas de capacitación del personal e intermediarios en materia de prevención de LA/FT/PADM.

61.4 Participar en el desarrollo y actualización de nuevos productos y procesos a fin de asegurar controles adecuados en relación al riesgo LA/FT/PADM.

61.5 Asegurar que el personal esté en conocimiento y aplique los procedimientos internos, de forma que todas aquellas transacciones que puedan ser consideradas como sospechosas o inusuales lleguen a su conocimiento para dar inicio al mecanismo de análisis y reporte de operaciones a la UIAF.

61.6 Actuar con objetividad e independencia en la planificación y ejecución de sus actividades.

62. La institución debe desarrollar un sistema que permita identificar, medir, monitorear y controlar el nivel de riesgo, alineado con las políticas definidas, y acorde con su tamaño, complejidad y riesgo de sus actividades, así como comprender una revisión y evaluación independiente sobre su idoneidad.

Para ello la institución debe:

62.1 Implementar un sistema que permita identificar su exposición al riesgo para los distintos productos, clientes, condiciones de contrato, canales de comercialización, métodos de pago y otros factores relevantes.

62.2 Diseñar procedimientos que contengan controles oportunos, efectivos y fáciles de implementar para todos los factores de riesgo definidos por la Dirección, los que deberán estar contenidos en un manual interno detallado, práctico y de fácil consulta, el que deberá mantenerse actualizado.

62.3 Diseñar procedimientos de debida diligencia diferenciales que permitan obtener un adecuado conocimiento de los clientes, que contemplen criterios de aceptación, requisitos de identificación y respaldo documental para aquellos de mayor riesgo. Estos procedimientos deberán considerar el tipo de cliente, el tipo de seguro a contratar, el volumen de los fondos involucrados y la evaluación de riesgo realizada por la institución.

62.4 Implementar procedimientos de monitoreo acordes con su tamaño, riesgo y complejidad de sus actividades que permitan detectar desvíos respecto de lo usual para el tipo de cliente, actividad u operación.

62.5 El sistema de monitoreo debe:

- Gestionar alertas en forma oportuna, requiriendo la información adicional que corresponda.
- Comprender un control contra listas de personas identificadas como terroristas confeccionadas en cumplimiento de la Resoluciones del Consejo de Seguridad de la Organización de Naciones Unidas o por

resolución Judicial Firme, así como con listas de personas que puedan estar vinculadas con actividades de lavado de activos o financiamiento del terrorismo.

63. La institución debe contar con procedimientos para detectar las operaciones inusuales y/o sospechosas, a efectos de notificar al supervisor y atender en forma oportuna sus solicitudes.

Para ello, debe:

63.1 Definir claramente el proceso para identificar, investigar y notificar transacciones sospechosas al supervisor y comunicarse a todo el personal. Estas definiciones deben incluir los canales internos de reporte, los responsables por el análisis y las guías a considerar.

63.2 Establecer un mecanismo que le permita asegurarse de detectar de forma rápida cualquier transacción vinculada directa o indirectamente con alguna de las personas u organizaciones incluidas en las listas confeccionadas a tales efectos.

63.3 Realizar un seguimiento de las transacciones realizadas, procediendo al análisis de aquellas que resulten inusuales, complejas o de gran magnitud, para permitir la detección de las que corresponden reportar a la UIAF.

RIESGO DE REPUTACIÓN

El riesgo de reputación se define como el riesgo presente y futuro de que las ganancias o el patrimonio de la entidad se vean afectados por una opinión pública negativa. Afecta la capacidad de la institución de establecer nuevas relaciones o servicios o continuar sirviendo las relaciones ya existentes. Este riesgo puede exponer a la institución a juicios, pérdidas financieras o a una disminución en la base de clientes. La exposición al riesgo de reputación incluye la responsabilidad de tener amplia precaución al tratar con los clientes y la comunidad.

El riesgo de reputación no es fácilmente cuantificable pero aparece en todas las relaciones con los clientes, en particular aquellas que aparejan asesoramiento y manejo de información confidencial de los mismos.

64. El Directorio debe aprobar y revisar periódicamente las políticas vinculadas al manejo de las relaciones con los clientes que consideren una gestión adecuada de las actividades de asesoramiento y la atención de reclamos por siniestros, ya sea directamente o a través de intermediarios y que incluyan formalmente el manejo de la información.

Para ello, el Directorio debe:

64.1. Aprobar las políticas en relación al riesgo de reputación. Estas políticas deben reconocer el riesgo de reputación que subyace en el relacionamiento con los clientes como un riesgo que la entidad debe manejar explícitamente. En este sentido, deben incluir elementos tales como la definición de la estructura y responsabilidades en el servicio de atención a los clientes, el sistema de reportes, la conservación de la documentación, entre otros:

64.2. Establecer políticas claras con relación a los clientes que incluyan:

- El trato a los mismos de forma justa procurándoles información oportuna y relevante sobre la cobertura del seguro que adquieren, sus derechos, obligaciones, primas y otros cargos a cobrar (sea en forma directa o a través de intermediarios).
- El establecimiento de un proceso formal para reclamaciones por siniestros.
- El tratamiento de la privacidad de la información de los clientes.

64.3. Cuando los intermediarios de seguros actúen en representación de la empresa e integren su fuerza de ventas, se deben establecer políticas claras de relacionamiento con los mismos que consideren:

- Los criterios de selección, conocimientos y capacidades requeridas y que cuenten con buena reputación.
- La capacitación en forma continua.
- La supervisión en cuanto a la aplicación de las políticas y procedimientos definidos, especialmente en lo referido a asesoramiento a los clientes, en particular la obligación de informar al cliente el rol que desarrolla, las características del producto comercializado y que la información entregada por el intermediario tiene los mismos efectos que la entregada por la propia aseguradora.
- La existencia de acciones correctivas.
- El régimen de retribución.

64.4. Establecer políticas claras de relacionamiento con terceros (proveedores más relevantes incluyendo tercerizaciones).

64.5 Promover una cultura ética en la institución donde se estipulen los principios y valores que rigen las actuaciones y los estándares de comportamiento ético que se espera de todos los integrantes de la organización, incluyendo su personal superior, a través de un Código Ética y que a su vez comprenda el relacionamiento con clientes, a través de un Código de Buenas Prácticas.

64.6 Considerar el riesgo reputación derivado de pertenecer a un conglomerado financiero, generado por la existencia de entidades subsidiarias y entidades vinculadas, según corresponda.

64.7 Asegurar el cumplimiento de las políticas definidas en relación al riesgo de reputación.

64.8 Revisar periódicamente la efectividad de estas políticas.

65. La Alta Gerencia debe implementar y comunicar las políticas definidas, asegurar que las mismas se cumplen y reportar al Directorio sobre el manejo de este riesgo.

Para ello, la Alta Gerencia debe:

65.1 Identificar adecuadamente las fuentes potenciales de riesgo de reputación y en consecuencia, se establecen mecanismos que mitigan o eliminan este riesgo.

65.2 Diseñar procedimientos para el adecuado asesoramiento a los clientes y la atención de reclamos.

65.3 Proveer entrenamiento continuo al personal relevante en esta tarea.

65.4 Asegurar que existen mecanismos de evaluación independientes de la efectividad de las políticas definidas en torno al relacionamiento con los clientes. Deberá incluirse la evaluación del funcionamiento del servicio de atención al cliente, en particular, la adhesión a las políticas y procedimientos definidos, la naturaleza y cantidad de reclamos recibidos y las operativas, productos o servicios que puedan presentar problemas extendidos de malas prácticas.

65.5 Considerar explícitamente el riesgo de reputación en el proceso de lanzamiento de nuevos productos u operativas.

65.6. Manejar los riesgos derivados de la administración de información sensible o confidencial por parte de intermediarios y proveedores de servicios tercerizados, cuando existan.

65.7 Designar un responsable del funcionamiento del servicio de atención de reclamos de clientes. Este servicio debe ser llevado adelante con independencia y objetividad, por personas que cuentan con la experiencia y conocimientos adecuados para ejercer estas funciones.

65.8 Asegurar que se aplican efectivamente los procedimientos de atención de reclamos establecidos.

65.9 Asegurar que los Códigos de Ética y de Buenas Prácticas aprobados son conocidos y aplicados por toda la organización y reflejan lo establecido en la normativa vigente.

65.10 Supervisar a los intermediarios para el cumplimiento de las políticas y procedimientos definidos.

65.11 Implementar una adecuada difusión del servicio de atención al cliente en las oficinas de la institución, en la documentación y en el sitio de Internet de la entidad.

65.12 Reportar al Directorio en forma periódica sobre cualquier aspecto que represente un riesgo de reputación significativo, en particular en lo que refiere a los resultados de la gestión del servicio de atención al cliente.

ESTÁNDARES DE TECNOLOGÍA (T)

Los estándares para la evaluación de las áreas de Tecnología de Información (TI) tienen como base el conjunto de principios conocido como COBIT en particular los vinculados al dominio de Construir, Adquirir e Implementar. Los restantes dominios han sido contemplados en los estándares de Gobierno Corporativo y de Riesgo Operacional.

66. El área o responsable de TI debe tener la habilidad para identificar las necesidades y para desarrollar, adquirir, instalar y mantener soluciones de TI apropiadas de acuerdo a las necesidades de la entidad.

Para ello debe:

66.1 Tener procesos para identificar necesidades e implementar, controlar y mantener soluciones de TI adecuadas. Esto incluye compras de hardware o software realizadas por el proveedor interno o externo de TI, desarrollo y programación realizado por la institución o un proveedor externo, compra de servicios a vendedores independientes, centros de procesamiento de datos vinculados a la institución o una combinación de estas actividades.

66.2 Implementar una metodología de desarrollo de sistemas de la institución que incluye un análisis y gestión adecuada de los riesgos tecnológicos asociados.

66.3 Implementar procesos que aseguren que se mejoran y reemplazan componentes de TI en forma prudente y dentro de un ambiente controlado.

El comportamiento en el desarrollo, adquisición y en el manejo de los riesgos asociados debe basarse en la evaluación de factores como:

- El nivel y calidad de la supervisión y soporte al desarrollo y adquisición de sistemas por parte de la dirección.
- La adecuación de las estructuras organizacionales y gerenciales para establecer conocimiento y responsabilidad por las iniciativas en materia de sistemas y tecnologías de TI.
- El volumen, naturaleza y extensión de la exposición al riesgo de la institución en el área del desarrollo y adquisición de sistemas.
- La adecuación de los estándares de desarrollo, ciclo de vida y programación de los sistemas de la institución.
- La calidad de las prácticas de administración de proyectos que son seguidos por los desarrolladores, operadores, nivel gerencial/propietario (entendiendo por propietario al usuario final dueño de la aplicación), vendedores independientes o proveedores vinculados (entendiéndose por proveedor vinculado a una empresa externa vinculada al grupo) de servicios de TI y los usuarios finales.
- La independencia de la función de aseguramiento de calidad y la adecuación de los controles sobre los cambios de programas.
- La calidad y exactitud de la documentación de los sistemas.
- La integridad y seguridad del software de red, de base y aplicaciones.
- El desarrollo de soluciones de TI que satisfagan las necesidades de los usuarios finales.
- El grado de compromiso del usuario final en el proceso de desarrollo de los sistemas.

66.4 Tener un proceso que comprende todas las fases necesarias para implementar un cambio de sistemas incluyendo investigación de las alternativas disponibles, selección de la opción más adecuada para la organización como un todo, conversión a un nuevo sistema o integración de un nuevo sistema con los existentes.

66.5 Evaluar en los proveedores externos de servicios de TI los aspectos vinculados a la calidad de las entregas de software y documentación, y a la adecuación de la capacitación proporcionada a los clientes.

66.6 Contar con una adecuada gestión de configuraciones y cambios donde se definen y controlan los componentes del servicio, desarrollo y de la infraestructura. Se debe asegurar la fiabilidad y precisión de los registros.